COMITÉ CONSULTATIF NATIONAL D'ÉTHIQUE
POUR LES SCIENCES DE LA VIE ET DE LA SANTÉ

COMITÉ NATIONAL PILOTE D'ÉTHIQUE DU NUMÉRIQUE

SYNTHÈSE DES CONTRIBUTIONS

Décembre 2019 – Juillet 2020

66, rue de Bellechasse 75007 Paris – 01 42 75 66 42
www.ccne.fr – contact@comite-ethique.fr

Une création dans un contexte numérique inédit

Le Comité national pilote d'éthique du numérique (CNPEN) a été mis en place en décembre 2019 à la demande du Premier ministre[1] et placé sous l'égide du Comité consultatif national d'éthique (CCNE). Il est constitué de 27 personnes issues d'horizons différents pour aborder de manière globale les enjeux d'éthique du numérique. Son rôle est à la fois d'élaborer des avis sur les saisines qui lui sont adressées et d'effectuer un travail de veille pour éclairer le débat public.

La crise sanitaire de la Covid-19, survenue peu de temps après sa création, a conduit à une intensification remarquable des usages du numérique pour informer, communiquer, surveiller, éduquer, travailler, prévenir et soigner, ou encore recueillir et exploiter des données - notamment durant la période de confinement.

Cette amplification a ouvert la voie à de nouvelles perspectives tout en mettant en évidence des questionnements organisationnels, techniques, sociétaux et économiques. Le CNPEN s'est autosaisi de ces enjeux et a mis en place, dès le début du confinement en France, un groupe de travail chargé de mener une veille sur les enjeux d'éthique soulevés par les usages du numérique en période de crise sanitaire aiguë. Il semblait en effet important de souligner des points de vigilance afin d'éclairer les décisions et de nourrir la réflexion relatives à l'usage du numérique dans les stratégies de gestion de la pandémie.

Cette crise initiée par la Covid-19 confirme l'importance de préserver les espaces de réflexion, d'échanges et de débats qui permettent de favoriser une attention à ces enjeux, de mettre en évidence des tensions éthiques, de nourrir le débat public et d'éclairer nos décisions individuelles et collectives.

Ce document rassemble les contributions du CNPEN dans ce contexte, depuis sa création jusqu'au mois de juillet 2020.

En parallèle de cette réflexion éthique conduite face à l'urgence, les quatre groupes de travail constitués dès le mois de janvier 2020 pour répondre aux saisines initiales du Premier ministre ont poursuivi leurs travaux. Nous présentons aussi ici leur état d'avancement.

***

[1] https://www.ccne-ethique.fr/fr/actualites/creation-du-comite-pilote-dethique-du-numerique

Les groupes de travail du CNPEN

Groupe de travail « COVID19 : enjeux éthiques soulevés par les usages du numérique en période de crise sanitaire aigue. »

Bien que la réflexion éthique relève plutôt du temps long, le CNPEN a estimé que la situation exceptionnelle liée au SARS-CoV-2 soulevait des questions éthiques immédiates liées à l'accroissement ou à l'évolution des usages du numérique. Il a donc décidé de s'autosaisir de ces enjeux. Cette veille a conduit à la publication d'un communiqué de presse relatif au suivi épidémiologique en sortie de confinement et de trois bulletins :

- le premier rassemble des points d'attention éthique relatifs d'une part à l'usage d'outils numériques dans le cadre d'actions de fraternité et d'autre part au suivi des personnes par des outils numériques.
- le deuxième traite des enjeux d'éthique dans la lutte contre la désinformation et la mésinformation.
- le troisième, élaboré en collaboration avec le CCNE, traite des enjeux d'éthique liés à l'usage d'outils numériques en télémédecine et télésoin dans le contexte de la COVID-19.

Suite à la saisine conjointe de messieurs les ministres Olivier Véran et Cédric O le comité a rendu un avis concernant l'usage d'outils numériques dans le cadre du déconfinement.

Groupe de travail « Véhicule autonome »

Ce groupe travaille en lien avec la Mission de madame Anne-Marie Idrac, Haute Responsable pour la stratégie nationale de développement des véhicules autonomes et le Grand Défi "Intelligence artificielle" du Secrétariat général pour l'investissement.

Il a déjà mené plusieurs auditions, notamment auprès de constructeurs, d'opérateurs ou encore de grandes métropoles comme celles de Lyon et Rouen où des expérimentations sont en cours.

Groupe de travail « Agents Conversationnels »

Le groupe de travail constitué pour répondre à la saisine du Premier ministre sur les agents conversationnels interroge les enjeux éthiques que peuvent soulever ces systèmes capables de communiquer avec un utilisateur humain par la voix ou par écrit. Ce groupe appuie sa réflexion sur les travaux menés sur ce thème au sein de la CERNA jusqu'en 2019.

Il a lancé en juillet un appel à contribution ouvert à tous jusqu'au 31 octobre 2020.

Groupe de travail « Diagnostic et Intelligence Artificielle »

La saisine a été précisée et le travail est en cours en collaboration avec le CCNE pour les sciences de la vie et de la santé.

Groupe de travail « Relations européennes et internationales »

Le groupe de travail sur les relations européennes et internationales a pour rôle de favoriser les échanges et les relations du CNPEN au-delà des frontières françaises. Il permet au comité de se tenir informé des réflexions existantes dans d'autres pays et d'organiser des échanges avec d'autres instances.

Il a préparé la réponse du Comité à la consultation ouverte par la Commission Européenne sur son *Livre blanc sur l'intelligence artificielle - Une approche européenne*.

Les membres du Comité national pilote d'éthique du numérique

Gilles Adda
Raja Chatila
Theodore Christakis
Laure Coulombel
Jean-François Delfraissy
Laurence Devillers
Karine Dognin-Sauze
Gilles Dowek
Valeria Faure-Muntian
Christine Froidevaux
Jean-Gabriel Ganascia
Eric Germain
Alexei Grinbaum
David Gruson
Emmanuel Hirsch
Jeany Jean-Baptiste
Claude Kirchner
Augustin Landler
Christophe Lazaro
Gwendal Le Grand
Claire Levallois-Barth
Caroline Martin
Tristan Nitot
Jérôme Perrin
Catherine Tessier
Serena Villata
Célia Zolynski

TABLE DES MATIÈRES

CRÉATION DU COMITE PILOTE D'ÉTHIQUE DU NUMÉRIQUE

Communiqué de presse
Publié le 2 décembre 2019

https://www.ccne-ethique.fr/fr/actualites/creation-du-comite-pilote-dethique-du-numerique

Une dimension nationale pour répondre à des enjeux éthiques majeurs

Le Comité Consultatif National d'Éthique pour les sciences de la vie et de la santé (CCNE) a été chargé par le Premier ministre de constituer un comité pilote d'éthique du numérique. Organisé sur le mode de fonctionnement du CCNE, ce comité pilote est constitué de personnalités d'horizons différents afin d'aborder de manière globale les enjeux éthiques du numérique et de l'intelligence artificielle. Ses premiers avis porteront sur les agents conversationnels, le véhicule autonome et le diagnostic médical à l'ère de l'intelligence artificielle. Il mettra également en place les moyens nécessaires à l'information et à la prise de décision individuelle et collective. Il tiendra sa première réunion plénière le 4 décembre 2019.

L'essor des sciences et technologies du numériques, leur diffusion massive et la rapidité avec laquelle elles se développent sont sources de transformations dans toutes les sphères d'activité, qu'elles soient publiques ou privées. Les enjeux éthiques qui en résultent concernent toutes les composantes de la société: sociales, sociétales, économiques, entrepreneuriales et individuelles.

Dans ce contexte, le Premier ministre a chargé le Comité Consultatif National d'Éthique pour les sciences de la vie et de la santé (CCNE) de constituer un comité pilote, dont l'objectif est « *à la fois de remettre des premières contributions sur l'éthique du numérique et de l'intelligence artificielle et de déterminer les équilibres pertinents pour l'organisation du débat sur l'éthique des sciences et technologies du numérique et de l'intelligence artificielle*». Cette initiative s'inscrit dans la stratégie nationale d'intelligence artificielle et dans la continuité des recommandations du rapport « *Donner un sens à l'intelligence artificielle* » de Cédric Villani et de l'Avis 129 du CCNE. Celui-ci proposait en effet, en septembre 2018, « *de jouer un rôle d'aide à la constitution d'un futur comité d'éthique du numérique, spécialiste des enjeux numériques dans leur globalité* ».

Constitué d'environ 30 personnes et dirigé par Claude Kirchner, Directeur de recherche émérite Inria, ce comité pilote, qui est placé sous l'égide du CCNE, va fonctionner sur le modèle de celui-ci. Pluridisciplinaire, il réunit des spécialistes du numérique, académiques ou issus des entreprises, des philosophes, des médecins, des juristes, des membres de la société civile ainsi que des membres du CCNE et de la CERNA[2]. Il associera dans les groupes de travail qui en seront issus des personnalités ayant une compétence dans les saisines traitées. Il a également pour mission de mettre en place les moyens nécessaires à la sensibilisation, à l'information et à la prise de décision

[2] CERNA : Commission de réflexion sur l'éthique de la recherche en science et technologies du numérique d'Allistene

des personnes, entreprises, administrations, institutions … Il travaillera en lien avec plusieurs organisations, notamment la CNIL, l'Inria, le CNRS, la CPU, les Académies des Sciences et des Technologies ou encore le CNNum[3], ainsi qu'avec des comités d'éthique français et étrangers. Le comité, qui est accueilli dans les locaux du CCNE – 66 rue de Bellechasse, Paris 7e – tiendra sa première réunion plénière le 4 décembre 2019.

Le comité pilote d'éthique du numérique portera ses premiers travaux sur trois saisines :

- *Les agents conversationnels* présents dans les téléphones, les interfaces avec les services en ligne ou encore les appareils domestiques tels les enceintes connectées. Les enjeux éthiques concernent la transparence sur le traitement des données récoltées, le respect des individus d'une part et la commodité de l'utilisation de telles applications de l'autre, ou encore la mise en œuvre de stratégies d'influence par de tels agents.

- *Le véhicule autonome* : le comité analysera les tensions existantes entre automatisation et maitrise humaine dans le contrôle du véhicule, ou encore les responsabilités partagées entre constructeur, assureur et utilisateur. Ces réflexions seront menées en lien avec la mission confiée à Mme Anne-Marie Idrac[4].

- Concernant enfin *le diagnostic médical et l'intelligence artificielle,* il s'agira de discuter la tension entre proposition de décision algorithmique et garantie humaine, de se demander quels sont les risques encourus lorsqu'on ne suit pas le « conseil » d'un algorithme de prédiction ou encore de promouvoir la transparence et l'explicabilité du fonctionnement de ces algorithmes tant pour les professionnels de santé que pour les usagers du système de santé.

Début 2021, le Comité pilote d'éthique du numérique remettra au Président du CCNE le bilan de ses activités. Le CCNE émettra ensuite des recommandations sur les modalités d'un éventuel comité pérenne d'éthique du numérique.

[3] CNIL : Commission nationale de l'informatique et des libertés,
Inria : Institut national de recherche dédié aux sciences du numérique,
CNRS : Centre national de la recherche scientifique,
CPU : Conférence des présidents d'université,
CNNum : Conseil national du numérique

[4] Nommée Haute responsable pour la stratégie nationale de développement des véhicules autonomes

THE FRENCH NATIONAL COMMITTEE FOR DIGITAL ETHICS

Présentation du Comité national pilote d'éthique du numérique
Publié le 24 février 2020

https://ai-regulation.com/the-french-national-committee-for-digital-ethics/

Digital Ethics places the human being and the human societies at the center of any reflection on innovation and its consequences in the digital sphere, including the use of information science, technology and artificial intelligence.

A national committee dedicated to Digital Ethics

In July 2019, the French prime minister assigned the president of the French National Consultative Committee on Bioethics (CCNE, created in 1983), the mission to launch a pilot initiative dedicated on Digital Ethics. This request came as an integral part of the French national strategy for artificial intelligence. It is in line with the recommendations of Cédric Villani's report "For a meaningful artificial intelligence, towards a French and European strategy". It also follows CCNE's Opinion 129 that proposed "to play a role in helping to set up a Digital Ethics committee focusing on issues in the field of information and communication technologies''.

This French National Committee for Digital Ethics (FNCDE) shall "submit initial contributions on the ethics of digital sciences, technologies, uses and innovations and determine relevant equilibria for the organization of public debate on digital ethics and artificial intelligence''. It was also given the task of raising awareness, informing and assisting individuals, companies, administrations, institutions, etc., in their decision-making process. FNCDE will work in conjunction with such stakeholders as CNIL (the French Data Protection Authority), Inria (the French Research Institute on Informatics and Applied Mathematics), CNRS (the French National Center for Science Research), French Universities, the French Academies of Science and Technology and the French National Digital Council. It will also liaise with other French and foreign ethics committees.

Placed under the CCNE aegis and hosted on its premises, FNCDE operates on a similar model. It has a pilot status and will propose a recommendation for the formation of a permanent body in early 2021. It is currently composed of 27 members from different disciplines: from IT specialists working in public or private research to philosophers, medical doctors, lawyers, and members of civil society. Workgroups tasked with preparing FNCDE opinions can include external experts.

The committee has already been seized by the Prime Minister to give opinions on the ethical issues concerning three specific topics of digital applications using in particular machine learning: 1) Conversational agents (chatbots); 2) Autonomous cars; and 3) Medical diagnosis and health AI. As the CCNE, the FNCDE can also seize itself on other topics, going beyond the topics submitted to it by the French Government.

Why Digital Ethics now?

Though it has taken millenniums to be recognized as such, information is now identified as important as matter, energy or life. The sciences and technologies of information have mainly been developed since the second half of the 20th century and they have profound consequences on humans because we are biological information processing systems, even if of course we are not only that. The biological information processing systems, that we are, and the digital ones, that we have developed, are interacting, collaborating and combining for the best but sometimes not for only that. This makes it crucial for all of us to think about the values that these uses and interactions carry. Thinking about our positioning on value hierarchies, along the way, based on experience as well as personal and collective reflection is central for ethics.

How the digital information processing systems we have developed and that are becoming more and more sophisticated are challenging such values as human dignity, privacy, empowerment, justice, fraternity, is becoming a key question. Digital Ethics is now a crucial issue in a global world where data, information and knowledge play such a central role is our daily life and in our societies. In this context the main goal of the FNCDE is to help organizing the thinking on Digital Ethics in France in strong coordination with European and international institutions and initiatives.

How the digital information processing systems we have developed and that are becoming more and more sophisticated are challenging such values as human dignity, privacy, empowerment, justice, fraternity, is becoming a key question. Digital Ethics is now a crucial issue in a global world where data, information and knowledge play such a central role is our daily life and in our societies. In this context the main goal of the FNCDE is to help organizing the thinking on Digital Ethics in France in strong coordination with European and international actions.

Digital Ethics for all

Ethical issues that are raised by the development of digital sciences, technologies, uses and innovations, concern everyone, even the “least-connected” of us. The digital evolution offers formidable opportunities at the individual and collective levels with deep impacts on humans and their organizations. Today to produce and supply electricity, to manage water, to design and operate airplanes, to communicate, photograph, talk to each other, etc., we make a strong and often very clever use of digital sciences and technologies. In this context, all machines, networks, protocols, algorithms and software at the kernel of the digital objects embed values and design choices: what are they? who has decided about their hierarchy? how are they implemented? Many situations that we can experiment every day when using a smartphone or when interacting with a digitalized administrative process make Digital Ethics a subject for everyone. Therefore, the second main goal of the FNCDE is to provide all society stakeholders with opinions to allow them to better understand issues and to help them making their own opinion. Finding appropriate ways to include all stakeholders in the elaboration of opinions is a challenge.

Digital Ethics, law and regulation

Ethics is not law and if the two are quite related, they might sometimes have complex relations and follow different paths that may lead to opposite views. Regulations and laws are designed at the political level in an independent way and the role of ethics in this context is to provide the legislator or the regulator with views, analyses and opinions on the ethical issues at stake. This rich and elaborated discussion between ethics and law is universal and not proper to the digital field. What makes in this context the originality of digital sciences and technologies is the current impressive speed of development as well as the specificity due to information processing. The fact that code is law, as seminally stated by Lawrence Lessig, so as the applications deployment speed towards

millions or even billions of humans or of digital devices, challenge regulators and legislators in multiple ways. In the digital domain particularly, the de facto standards impose themselves on normalization, regulation and even law. In this context, ethics shall provide the legislator and the regulator with reflection and value-based analyses of the systems and their potential uses. In particular the FNCDE intends to enlighten the French legislators or regulators and to be useful to European and international debates on these issues.

Digital Ethics at the European and World levels

The development of the digital technologies, based in particular on the internet and, at least initially, on the net philosophy promoting the universal ease of communication and sharing of information, tends to make geographical frontiers disappear. From the historical notion of national sovereignty, we come to new notions of strategic autonomy, including individual or technological, digital, economical, educational, etc., sovereignties. Digital Ethics as well as laws or regulations cannot escape from this globalization trend anymore. The FNCDE shall therefore work in collaboration with similar committees in other countries, building on shared grounds. Contacts have already been established with several institutions.

Thinking globally

The French National Committee for Digital Ethics is a great opportunity resulting from multiple good wills and that challenges us to demonstrate its interest and usefulness. The FNCDE will interact with various stakeholders, including the industry and the civil society, and will undertake a series of hearings and consultations in order to prepare its Opinions. Its creation in the context of the CCNE, which has a long experience dealing with tough ethical issues, is a chance: sharing competences, know-how and means benefits to both committees. This also favors cross-fertilization and joint initiatives, in particular towards education of all people from kindergarten to seniority. It challenges us also in understanding how a global thinking on ethics could be organized at the level of our country. This involves obviously the health and digital fields, but also environmental issues or other main topics that are questioned by the strong evolutions of our human societies. The next two years of FNCDE, in strong cooperation with CCNE and many others institutions at the French, European and international levels will help to elaborate answers and actions addressing the various issues mentioned in this overview. The active contributions of all, in this dynamic and challenging context, are particularly welcome.

RÉFLEXIONS ET POINTS D'ALERTE SUR LES ENJEUX D'ÉTHIQUE DU NUMÉRIQUE EN SITUATION DE CRISE SANITAIRE AIGUË

Bulletins de veille

Bulletin de veille n°1 :

FRATERNITE : POINTS D'ATTENTION ETHIQUE SUR LES OUTILS NUMERIQUES

et

LE SUIVI DES PERSONNES PAR DES OUTILS NUMERIQUES

Bulletin de veille
Publié le 7 avril 2020

https://www.ccne-ethique.fr/fr/actualites/comite-national-pilote-dethique-du-numerique-bulletin-de-veille-ndeg1

Le Comité national pilote d'éthique du numérique a été mis en place en décembre 2019 sous l'égide du Comité consultatif national d'éthique (CCNE) à la demande du Premier ministre[5]. Il est constitué de 27 personnes d'horizons différents, issues du monde académique, des entreprises ou de la société civile, pour aborder de manière globale les enjeux d'éthique du numérique. Son rôle est à la fois d'élaborer des avis sur les saisines qui lui sont adressées et d'effectuer un travail de veille pour éclairer les prises de décision individuelles et collectives.

C'est ce travail de veille nécessité par l'urgence et l'importance de la crise Covid-19 que nous exposons ici. En concertation étroite avec la veille menée par le CCNE sur les enjeux de bioéthique et sans omettre la dimension européenne et internationale, il s'agira d'identifier les questions éthiques soulevées par les usages du numérique dans cette situation de crise. Nous souhaitons exposer et discuter les dilemmes posés par les mesures qui pourraient être autorisées pour tenir compte des impératifs de santé publique et dérogeraient aux valeurs fondamentales partagées dans notre société. Nous analyserons également comment, en sortie de crise, nous pourrons assurer un retour à une situation conforme à ces valeurs. En effet, cette épreuve surmontée, les choix collectifs et individuels réalisés maintenant pour permettre de la résoudre affecteront nos vies pour les années à venir.

La pandémie du Covid-19 nous touche tous. Si nous estimons qu'il est fondamental de conduire une veille éthique sur les usages du numérique, nous pensons avant tout aux personnes en difficulté, dans la maladie, ou dans le deuil, aux soignants, aux accompagnants, à l'ensemble de nos concitoyens qui se mettent au service de la collectivité pour lui permettre de passer cette épreuve. Nous élaborerons nos recommandations en étant conscients de leurs souffrances, de leurs difficultés, et de l'importance de leur dévouement. Nous espérons que chacun pourra s'en faire un point d'appui dans l'instant et pour le futur.

Claude Kirchner
Directeur du comité national pilote d'éthique du numérique

[5] https://www.ccne-ethique.fr/fr/actualites/creation-du-comite-pilote-dethique-du-numerique

L'OBJECTIF DES BULLETINS DE VEILLE

La réflexion éthique relève du temps long. Cependant le comité a estimé que la situation exceptionnelle de la crise sanitaire actuelle soulevait des questions éthiques immédiates liées à l'accroissement ou à l'évolution des usages du numérique, dont il a décidé de s'auto-saisir[6]. Ces questions sont explicitées de manière synthétique ci-dessous. Elles ne sont pas toutes nouvelles mais se trouvent considérablement amplifiées et de ce fait, appellent à une vigilance renforcée. D'autres sujets sont susceptibles de surgir en fonction de l'évolution de la pandémie et de nouveaux usages du numérique.

Au-delà de notre démarche, il nous semble important de réfléchir à ces questions en associant toutes les composantes de notre société et tout particulièrement de faciliter l'implication citoyenne.

Sur les usages du numérique relatifs à la gestion de la pandémie

Les technologies numériques sont utilisées massivement en cette période de crise sanitaire, avec des bénéfices immédiats pour la gestion de la pandémie elle-même.

En ce qui concerne le soin, l'usage renforcé de la télémédecine et des outils de communication numériques permet le maintien de la relation entre les soignants et les patients, quel que soit l'objet de la consultation. Se posent cependant des questions relatives tant à la nature, la sécurité et à la confidentialité des échanges entre le médecin et le malade, qu'aux évolutions de la médecine libérale que cela risque d'induire, avec le développement des plates-formes privées.

En matière de santé publique, la gestion de la crise pourrait entraîner la mise en œuvre d'une stratégie de suivi numérique de l'état sanitaire de la population. Ce point est développé dans la seconde partie de ce bulletin.

En ce qui concerne la recherche, les données, modèles, protocoles et algorithmes disponibles – grâce en particulier au libre accès aux publications scientifiques – permettent d'aider au diagnostic, de calculer des statistiques, d'élaborer des prévisions et de tirer des leçons des stratégies mises en œuvre dans différents pays. Toutefois, il convient de prendre conscience du contexte d'incertitude et d'urgence dans lequel les résultats et retours d'expérience sont considérés et de s'assurer de leur assise scientifique.

Sur les usages du numérique concernant les personnes

L'ensemble de la population est également appelé à utiliser les outils numériques de manière plus intensive, que ce soit pour le télétravail, l'éducation et la formation, l'information, la culture et les loisirs. Plus généralement, ces outils permettent d'assurer la continuité du lien social et suscitent de nouvelles formes de solidarité.

Cependant, tous les métiers ne se prêtent pas au télétravail, ce qui engendre des disparités et inégalités : par la nature de leur profession, certaines personnes ne peuvent poursuivre leur activité tandis que d'autres doivent la poursuivre avec un risque de contamination.

En ce qui concerne les prestations proposées via le numérique (prestations culturelles, sportives, etc.) et permettant un mieux-vivre pendant la période de confinement, une

[6] Voir l'auto-saisine en annexe

réflexion devrait s'engager sur les différentes formes de reconnaissance des acteurs impliqués.

La multiplication des échanges à travers des terminaux modifie les liens sociaux. Si les systèmes de vidéo ou d'audio conférence, les plates-formes de télé-enseignement, les agents conversationnels, sont particulièrement utiles en temps de crise sanitaire, il faut s'interroger sur l'accoutumance à certains usages numériques, envisager leur irréversibilité, qui conduiraient à une évolution des modes de vie. Par ailleurs, si le numérique permet la diffusion et la propagation rapides d'informations il facilite aussi la prolifération de fausses informations en particulier *via* les réseaux sociaux.

Il est à noter que face à ces usages intensifiés, les inégalités numériques, qu'elles soient d'ordre géographique, économique ou culturel, se trouvent renforcées, rendant les inégalités sociales encore plus importantes.

Sur les aspects techniques du numérique

L'intensification soudaine du recours à des technologies numériques ouvre la voie à de nouvelles perspectives tout en mettant en évidence ou en exacerbant des vulnérabilités techniques, organisationnelles et économiques.

L'usage massif d'outils de communication en ligne dans un cadre professionnel, familial et amical permet de maintenir des liens indispensables, mais soulève des problèmes majeurs en termes de sécurité, de confidentialité des propos échangés, et de souveraineté. D'autre part, si des ressources liées au numérique venaient à être limitées, la question de priorités entre usages selon leur « importance » pourrait également se poser.

La fermeture de commerces « non essentiels » a renforcé le commerce en ligne qui certes, aide à la continuité des approvisionnements et peut bénéficier à certains acteurs locaux, mais augmente aussi le pouvoir de géants du numérique qui, d'une certaine façon, bénéficient de la crise.

Enfin, on pourrait désirer que les systèmes de production et de services soient plus largement automatisés afin de pouvoir assurer la continuité des activités tout en préservant les salariés (caisses automatiques, usines entièrement robotisées, véhicules de livraison autonomes, etc.). Il faut cependant s'interroger dès à présent sur la mutation sociétale que la généralisation de ces innovations engendrerait à terme.

Dans ce cadre, ce premier bulletin de veille relatif aux enjeux éthiques du numérique en situation de crise sanitaire aiguë est consacré d'une part à la question de la fraternité s'appuyant sur des outils numériques, et d'autre part à la question du suivi des personnes par des outils numériques.

FRATERNITÉ : POINTS D'ATTENTION ÉTHIQUE SUR LES OUTILS NUMÉRIQUES

A. De la sidération au sursaut

Après une brève phase de sidération et de repli sur soi qui a entraîné une fermeture de nombreux lieux d'accueil et la suspension de la vie associative et des réseaux d'entraide, on a vu fleurir nombre d'initiatives de solidarité s'adaptant aux mesures de confinement, aux gestes-barrière et à l'exigence d'attestations de déplacement dérogatoire. Émanant d'individus, de groupes de voisinage, d'associations, d'institutions et de municipalités, ces initiatives ont rencontré un bel élan de fraternité intergénérationnelle, essentiellement grâce au téléphone portable, à internet, aux réseaux sociaux et aux plates-formes numériques. Le gouvernement accompagne cette mobilisation via le site https://covid19.reserve-civique.gouv.fr/et *#jeveuxaider* de la Réserve civique[7]. Il soutient aussi le site https://solidarite-numerique.fr.

On ne peut que se réjouir de ce sursaut fraternel qui appelle cependant quelques points d'attention sur les problématiques éthiques liées à l'utilisation d'outils numériques. Il s'agit en particulier de l'attention portée au respect de la dignité humaine, au principe d'équité dans la distribution des ressources, à l'autonomie de la personne, et à l'exigence de solidarité qui ont été rappelés dans un récent avis du CCNE [8], auxquels il convient de rajouter ici la bienfaisance et la non-malfaisance ainsi que le respect de la vie privée.

Solidarités avec qui et comment

Soignants et catégories professionnelles les plus exposées

Une des manifestations les plus visibles et audibles de la fraternité avec les personnels soignants fut l'initiative *#OnApplaudit*, lancée *via* les réseaux sociaux, appelant à exprimer son soutien en se mettant à sa fenêtre pour les applaudir chaque jour à 19h ou à 20h. De manière plus discrète on a vu naître des initiatives d'entraide locale pour la garde des enfants, les courses, voire l'hébergement près des hôpitaux. Cette forme de solidarité s'est étendue aux pompiers, ambulanciers, gendarmes et policiers, mais aussi aux professions assurant la continuité des activités considérées comme essentielles : éboueurs, caissiers, postiers, facteurs, routiers, camionneurs, livreurs, techniciens de maintenance, etc.

En outre pour aider les soignants à l'hôpital, des plates-formes numériques ont été créées pour affecter les renforts à différents postes dans les hôpitaux, et pour proposer des repas aux soignants en collaboration avec des restaurateurs.

Personnes vulnérables

Les personnes isolées, âgées et/ou handicapées, se trouvent confinées dans des institutions ou à domicile, coupées de leurs proches ou des bénévoles d'associations qui sont empêchés de venir leur rendre visite ou tenus de limiter leurs déplacements. Les institutions, comme les familles, les associations et les services d'aide à domicile font preuve d'inventivité pour maintenir des relations quasi-quotidiennes avec ces personnes.

---

[7] La réserve civique, instituée en France par la loi Égalité et Citoyenneté du 27 janvier 2017, permet l'engagement bénévole et occasionnel de citoyens pour des projets d'intérêt général.

[8] « COVID'19 : Avis du Comité Consultatif National d'Ethique : Enjeux éthiques face à une pandémie, réponse à la saisine du ministre en charge de la santé et de la solidarité », CCNE, 13 mars 2020 – www.ccne-ethique.fr

On peut se passer d'outil numérique quand il s'agit de téléphoner, écrire, voire prier, ce qui permet à des personnes peu à l'aise avec ces outils d'y participer et de se sentir utiles. Mais les interfaces numériques de communication, écrans, webcams, ou robots de téléprésence, sont de plus en plus répandues, par exemple dans les EHPAD. Elles peuvent répondre au droit au maintien d'un lien social pour les personnes dépendantes que vient de rappeler le CCNE [9]. Les usages de ces outils numériques pour communiquer avec les personnes malades ou en fin de vie posent néanmoins des problèmes éthiques par exemple liés au respect de la sphère intime.

Personnes en situation de précarité

Les personnes sans domicile fixe ou ne disposant que de faibles revenus ont été soudainement privées d'accès à des lieux de ressources alimentaires ou d'hygiène (toilettes, douches) ou d'accès à internet dans des accueils de jour, perdant parfois les revenus de petits services d'aide à domicile, voire le recours à la mendicité. Fort heureusement, grâce au numérique, plusieurs initiatives d'organismes publics et d'associations ont permis de rouvrir des services interrompus et de créer des services d'exception pour l'hébergement, l'aide alimentaire et l'hygiène. Cependant l'enjeu est alors l'accès des potentiels bénéficiaires à ces informations numériques. Dans les familles, particulièrement celles vivant dans des conditions difficiles, les enfants sont aussi pénalisés par des inégalités d'accès et d'accompagnement au télé-enseignement. De nombreux enseignants actifs ou retraités se mobilisent pour les aider *via* les réseaux sociaux. L'exiguïté des logements est aussi génératrice de violences familiales qui touchent principalement les femmes et les enfants. Là encore des initiatives de solidarité qui se mettent en place sont relayées par des outils numériques.

Accès aux outils numériques

L'accès aux outils numériques, en particulier à internet, est essentiel dans la mise en œuvre d'initiatives de solidarité dans la situation de crise que nous vivons. Par exemple, des applications accessibles sur *smartphone* ont été spécialement conçues pour informer les personnes en situation de précarité, les mettre en relation et renforcer ainsi leur autonomie.

Encore faut-il une équité d'accès à ces outils tant pour les personnes voulant se rendre solidaires que pour celles qui en sont les destinataires. Or les personnes en précarité ont souvent des abonnements limités pour leur *smartphone* quand elles en disposent. Dans les familles, les postes de travail informatique à domicile pour le télé-enseignement ne sont pas toujours disponibles ou bien équipés. Quant aux personnes isolées chez elles, elles subissent le stress de ne pouvoir accéder à des services ou des informations parce qu'elles ne maîtrisent pas l'accès à internet.

La bande passante de télécommunication pouvant devenir une ressource rare, il faut envisager l'arbitrage de son allocation sans pénaliser la solidarité qui doit être considérée comme une des activités essentielles en période de crise.

[9] « Réponse à la saisine du ministère des solidarités et de la santé sur le renforcement des mesures de protection dans les EHPAD et les USLD », CCNE, 30 mars 2020 – www.ccne-ethique.fr

Recommandations

- Aux opérateurs de télécommunications :
  - veiller à débrider les abonnements à faible capacité en période de crise.

- Aux municipalités :
  - mettre à disposition des outils numériques adaptés dans des lieux sécurisés et assister les usagers, et les maintenir après la période de crise.

- Aux services publics :
  - conserver une assistance téléphonique humaine pour suppléer aux difficultés d'accès aux services numériques et la maintenir après la période de crise.

- Aux services de l'État :
  - prévoir un canal de télécommunication « fraternité» prioritaire sur d'autres usages en cas d'arbitrage de l'allocation du réseau de télécommunication en période de crise.

Usage des interfaces de communication

Les interfaces numériques de communication visuelle et auditive, écrans, webcams, et robots de téléprésence permettent aux personnes isolées, malades ou âgées de maintenir le lien, encore plus indispensable en situation de crise, avec leurs proches.

Outre l'accès à ces outils, des questions éthiques spécifiques se posent quant à leur emploi et à l'enregistrement d'images ou de conversations, en général et d'autant plus dans des situations extrêmes, en réanimation ou en fin de vie. La téléprésence peut alors engendrer un choc psychologique pour les patients de voir leurs proches seulement à distance, ou pour les proches de voir le patient souffrir et en situation de faiblesse. Quant aux images ou sons enregistrés, ils peuvent être considérés comme attentatoires à la dignité et au respect de la vie privée de la personne souffrante. *A contrario* en cas de décès, l'absence d'image, à défaut d'une présence physique, peut être un obstacle douloureux pour faire ultérieurement son deuil. Pour garantir la non-malfaisance de ces interfaces numériques, il semble donc nécessaire de prévoir un accompagnement dans leur choix et dans leur mise en œuvre, et une procédure relative à l'effacement ou à la conservation de ces enregistrements.

Recommandations

- Aux institutions accueillant des personnes vulnérables et éventuellement au législateur :
  - instaurer un rôle de médiateur de communication entre une personne âgée ou malade et ses proches via des interfaces de communication maîtrisées.
  - demander le consentement préalable au choix des interfaces et des modalités de communication, de la personne, de son éventuelle tutelle, curatelle, ou personne de confiance avant leur mise en œuvre.

- prévoir des procédures de discernement et de décision sur la conservation ou l'effacement des images, sons ou conversations enregistrées avec des personnes vulnérables.

- A l'ensemble de la population :
  - utiliser les interfaces numériques dans le respect de la dignité des personnes concernées, en veillant à ne pas les substituer à une présence physique une fois la période de confinement terminée.
  - s'interdire la diffusion sur les réseaux sociaux d'images de patients en fin de vie.

Usage des réseaux sociaux

Les réseaux sociaux jouent un rôle majeur dans l'émergence d'initiatives locales de solidarité visant en particulier les trois types de destinataires envisagés : soignants et catégories professionnelles exposées, personnes vulnérables et personnes en situation de précarité. Par leur agilité, ils ont l'avantage indéniable de la réactivité et de la rapidité de mise en œuvre des initiatives.

La contrepartie est la propagation d'informations incomplètes ou fausses qui peuvent affecter les actions de solidarité elles-mêmes de deux manières opposées. Une sous-estimation des risques pour les personnes exposées par des recommandations d'alimentation ou d'hygiène inopérantes voire présentant un danger pour la collectivité. *A contrario*, une surestimation des risques, au-delà des gestes-barrière préconisés, peut conduire à refuser toute forme de solidarité concrète ou stigmatiser des catégories de la population.

De plus, en situation de crise, les réseaux sociaux peuvent laisser des traces d'affichage de la vulnérabilité de certaines personnes, traces qui peuvent ensuite pénaliser leurs relations sociales par leur caractère discriminatoire.

Enfin certaines initiatives de solidarité diffusées par les réseaux sociaux peuvent être instrumentalisées par des intérêts sectaires[10] ou criminels. Europol signale des phénomènes de cybercriminalité exploitant spécifiquement la crise sanitaire et l'anxiété de la population[11].

Ces constats appellent donc des recommandations pour la bienfaisance et à l'exigence de solidarité dans l'usage des réseaux sociaux en temps de crise, ainsi qu'au respect de la dignité et de la vie privée au-delà de la crise.

Recommandations

- Aux pouvoirs publics :
  - continuer de faire relayer au sein des réseaux sociaux et par leurs principales applications des messages concernant les gestes-barrière.

[10] Anne-Marie Courage : « Le phénomène sectaire à l'heure du numérique », *BulleS* - N° 143 (2019) pp. 9-15

[11] « Pandemic profiteering how criminals exploit the COVID-19 crisis», EUROPOL, mars 2020 – www.europol.europa.eu

- Aux utilisateurs des réseaux sociaux :
  - vérifier que le réseau social utilisé a une politique claire et affichée de respect des données personnelles.
  - veiller aux risques de désinformation en ligne concernant l'épidémie de Covid-19, y compris en ce qui concerne les actions de solidarité.
  - être vigilant face aux risques d'escroquerie numérique exploitant l'élan de solidarité.

Usage des moteurs de recherche et des plates-formes

Les moteurs de recherche et les plates-formes numériques jouent un rôle fondamental dans la mise en relation des bénévoles et des associations ou des institutions proposant des actions de solidarité, mais aussi des entreprises proposant des produits ou des services pouvant contribuer à la solidarité nationale. On constate aussi un foisonnement de plates-formes d'innovation en open source pour inventer de nouveaux types de matériels médicaux, des traitements, ou tout simplement de nouvelles applications utiles en ces temps de pandémie.

À cet égard, on relève deux points d'attention. Le premier n'est pas nouveau ; il a trait au respect de la vie privée, mais il appelle une attention particulière s'agissant de bénévoles. Le second, spécifique à la crise, touche à l'équité dans le partage des fruits de la solidarité nationale.

L'afflux des candidats bénévoles sur des plates-formes génère des données personnelles qui sont stockées par les moteurs de recherche et les plates-formes qui pratiquent le traçage. Ces données peuvent être exploitées ultérieurement par opportunisme commercial ou de manipulation à l'insu des personnes qui dans l'urgence et l'absence d'éducation appropriée au numérique auraient pu donner trop rapidement leur consentement.

Tant la gestion des dons de matériels sanitaires et de produits de différentes natures et provenances que leur distribution aux personnels soignants et aux professions les plus exposées se sont avérées souvent chaotiques et inadéquates. À cela s'ajoutent les risques de contrefaçons exploitées par la cybercriminalité. Une plate-forme publique mettant en relation les offres et les besoins permettrait de se prémunir de ces aléas.

Recommandations

- Aux organisations caritatives et à tous les acteurs de la solidarité :
  - favoriser l'usage de moteurs de recherche et de plates-formes numériques garantissant la protection des données personnelles et un référencement utile des associations et des institutions dignes de confiance.

- Aux plates-formes numériques :
  - s'engager à l'effacement, à l'issue de la crise, des données collectées sur les bénévoles et les personnes aidées.

- Aux services de l'État :
  - privilégier des solutions numériques souveraines pour la gestion logistique tout particulièrement en période de crise.
  - créer une plate-forme publique mettant en relation les offres et les besoins.

Conclusion

Le présent constat sur l'accès aux outils numériques et leurs usages dans l'exercice de la fraternité et sur les enjeux éthiques associés est fait dans le contexte national de l'épidémie de Covid-19. Il est focalisé sur des solidarités concrètes vis-à-vis de trois catégories de la population dans cette période de crise et ne renvoie donc pas une image exhaustive de l'ensemble des actions de fraternité et des solidarités. Plusieurs thèmes n'ont pas été abordés, notamment ce qui concerne d'autres catégories de la population, tels que les migrants ou les détenus, et la dimension internationale de la solidarité n'a pas été prise en compte. Ceci appelle des analyses ultérieures.

LE SUIVI DES PERSONNES PAR DES OUTILS NUMÉRIQUES

Les technologies numériques concourent aux objectifs de santé publique et à la gestion de la crise sanitaire.

Les mesures de suivi numérique peuvent aider à lutter contre l'épidémie au niveau d'une population ou au niveau individuel. Au niveau collectif, elles peuvent notamment permettre d'étudier et de modéliser la propagation de l'épidémie, d'identifier les foyers d'épidémie, de contribuer à l'évaluation de l'immunité de la population et d'analyser l'effet du confinement. Au niveau individuel, elles peuvent permettre de suivre et de contacter les porteurs du virus et les personnes ayant été en contact avec eux, de veiller au respect du confinement et prévenir les attroupements non-autorisés, et de réduire la charge psychologique sur les personnes en leur fournissant des indications relatives à leur état de santé. Elles peuvent permettre également de faciliter le suivi médical des patients dans le respect des principes de bienfaisance, non malfaisance, justice et autonomie.

Dans le même temps, la gestion de la crise se retrouve en tension avec le respect des libertés fondamentales. Ainsi, le confinement des populations restreint la liberté de circulation ; les mesures de suivi numérique posent la question d'atteintes à la protection de la vie privée et des données personnelles. Le suivi de la distribution géographique des membres d'un groupe pourrait encore poser la question d'une discrimination éventuelle à leur égard même en cas d'utilisation des données agrégées. Même en situation de crise, il est nécessaire de définir des garde-fous solides et des limites à ne pas franchir. Toute mesure prise doit être guidée par le respect des principes fondamentaux parmi lesquels la nécessité, la proportionnalité, la transparence et la loyauté.

La réflexion éthique vise à identifier les tensions qui émergent entre les différents principes, entre les valeurs individuelles et collectives, le bien-être individuel et collectif, afin d'éclairer les citoyens et d'aider aux décisions de politique publique.

I. Enjeux éthiques de différents types de suivi numérique

Le suivi collectif concerne des groupes de population identifiés selon des critères variés, par exemple géographiques (toutes les personnes qui se retrouvent à un endroit particulier à un moment donné, ou les mouvements de populations), ou des critères de santé, de vulnérabilité, etc.

Le suivi individuel concerne les personnes elles-mêmes. Celles-ci pourraient inclure l'ensemble de la population, les personnes testées positivement, les personnes qui présentent des symptômes compatibles avec ceux de la maladie, les personnes ayant été en contact ou à proximité physique de personnes testées positivement, ou les contacts enregistrés dans le carnet d'adresses d'une personne.

Les moyens de suivi individuel pourraient être mis en œuvre de manière obligatoire ou sur une base volontaire. Ils poseraient en outre la question de l'obligation des personnes de rester connectées en permanence.

Dans le cas du suivi obligatoire, seraient invoqués l'urgence des mesures, les impératifs de santé publique ainsi que le besoin de toucher une plus grande partie de la population. Cependant, des mesures imposées pourraient produire un effet inverse à celui qui est visé en induisant des comportements de désaccord, par exemple la déconnexion du système de suivi durant les déplacements.

Dans le cas du suivi volontaire, l'adhésion libre serait encouragée par une information au public sur l'utilité du suivi et par un appel au sens civique, une incitation sociale, par exemple par envoi de SMS et de messages publics. Le principe d'équité supposerait alors que des dispositifs connectés spécifiques soient fournis aux personnes qui souhaiteraient adhérer aux mesures volontaires de suivi mais ne possèdent pas d'outil approprié.

Cependant, ce choix individuel peut être orienté, voire influencé, de diverses manières, par exemple à travers les techniques de persuasion (« *nudging* ») ou de manipulation, la pression sociale, l'imitation des actions des proches, etc. En pareille hypothèse, le défaut de consentement libre et éclairé, la possibilité de son instrumentalisation ainsi que la portée du consentement sur les proches et autres contacts de la personne concernée, ou encore l'attribution de la responsabilité à la personne plutôt qu'à la collectivité, sont d'importants sujets de préoccupation éthique. Comme le Comité consultatif national d'éthique l'avait relevé dans ses avis sur le numérique en santé, la préservation de l'autonomie de décision de la personne et la mise en œuvre d'une garantie humaine de ces technologies numériques représentent deux leviers essentiels de régulation, y compris en temps de crise.

MOYENS DE SUIVI

2.1 Les données de géolocalisation collectées à partir de dispositifs connectés.
2.2 Les données de géolocalisation des utilisateurs collectées par les opérateurs des publicités, les réseaux sociaux, les moteurs de recherche ou autres opérateurs de contenus en ligne fréquemment consultés.
2.3 Les données de proximité collectées par une application installée sur les dispositifs connectés.
2.4 Les données de vidéosurveillance de l'espace public (caméras, drones, robots), éventuellement couplées avec des systèmes de reconnaissance faciale.
2.5 Les données d'utilisation des cartes bancaires.
2.6 Les données d'activité des téléphones et des dispositifs d'accès à internet.
2.7 Les données de la consommation électrique.
2.8 Les données de santé collectées par des dispositifs médicaux connectés, par exemple les thermomètres.
2.9 Les données de santé collectées par les services de soin.
2.10 Les observations globales par drones ou satellites.

<u>Recommandation</u>

- En cas de mesures volontaires de suivi numérique, garantir le consentement libre et éclairé des personnes concernées.

La temporalité est également un enjeu fondamental : les mesures de surveillance numérique pourraient s'appliquer pendant la période de confinement ou après la levée de celui-ci, voire être appliquées à l'avenir en prévision de situations similaires.

Pour distinguer ces trois temps, la définition de la fin de l'urgence sanitaire et celle de la sortie de crise sont déterminantes. Ces définitions sont nécessaires pour fixer légalement la durée des mesures de suivi afin qu'elle soit la plus limitée possible au regard des finalités poursuivies. Le risque est en effet que ces mesures d'exception s'installent dans la durée. L'histoire comporte de nombreux exemples de mesures mises en œuvre de manière exceptionnelle, qui se sont ensuite prolongées, jusqu'à être intégrées dans le droit commun. On peut en outre redouter la tentation de pérenniser certaines formes de suivi. Dans cette hypothèse, la banalisation du suivi individuel constituerait un problème éthique important.

Recommandations

- Pour toute mesure de suivi, définir et annoncer une durée légale strictement limitée et garantir les conditions de sa réversibilité.
- Sur le plan technique, ne pas recourir à la prolongation automatique des autorisations de suivi. Prévoir la désactivation automatique des mesures de suivi individuel après l'expiration du délai légal ainsi que les moyens d'en rendre compte publiquement.

Assurer la robustesse, la sécurité, la traçabilité, l'explicabilité et l'auditabilité des mesures de suivi est un enjeu de premier plan. Par exemple, le recours aux moyens tels que le chiffrement ou les vérifications croisées concourt à la qualité technique du suivi. Quels que soient ces moyens, la précision des données et les méthodes de traitement sont toutefois susceptibles d'induire des erreurs d'interprétation, par exemple des « faux négatifs » ou « faux positifs ». Le respect de l'autonomie des personnes et des droits fondamentaux, principes éthiques autant que juridiques, impliquerait la possibilité de signaler une erreur et de recevoir une réponse, voire d'initier un recours en cas de préjudice subi, et en cas d'adhésion volontaire la possibilité de retrait et d'effacement des données collectées.

Un risque de discrimination sociale, voire de stigmatisation, peut émerger envers les personnes signalées par les applications de suivi. Ce risque concerne également les personnes qui n'ont pas adhéré aux mesures de suivi.

Un autre enjeu est celui du choix, collectif ou individuel, des mesures de suivi dans un contexte de multiplication des applications proposées par des acteurs privés ou internationaux licites ou illicites, ainsi que la collecte des données par ces différents acteurs.

Recommandations

- Évaluer la nécessité et proportionnalité des mesures à des intervalles réguliers. Définir les critères d'efficience des mesures et les évaluer de manière régulière.
- Au vu du caractère intrusif et massif des mesures de suivi, mettre en œuvre les moyens spécifiques et adaptés pour garantir leur sécurité et prévenir tout mésusage.
- Permettre aux personnes de signaler une erreur, de recevoir une réponse à leur requête et d'initier un recours en cas de préjudice subi.
- En cas d'adhésion volontaire, permettre aux personnes de revenir sur leur engagement et permettre l'effacement des données collectées.
- Les applications spécifiques de suivi doivent être certifiées par les autorités publiques et soumises à l'audit.

II. Enjeux éthiques de la collecte de données personnelles dans le cadre du suivi numérique

La collecte et le traitement des données personnelles, quelles que soient leurs sources, pourraient être utiles pour assurer un suivi efficace de la crise, par exemple en contribuant à identifier les personnes à risque, ainsi qu'à des fins de recherche scientifique, notamment en vue d'améliorer les politiques de prévention d'éventuelles pandémies futures.

Toutefois, cela peut présenter des risques d'atteintes disproportionnées aux libertés fondamentales, à un degré variable selon les mesures mises en œuvre. Par exemple, même les déplacements relevant de l'intimité de la vie d'une personne pourraient être analysés.

Les textes actuels prévoient d'ores et déjà leur application en temps de crise (v. article 23 du RGPD[12] et article 15 de la directive « Vie privée et communications électroniques ») en fixant les conditions de validité des dérogations au droit commun dans le respect des droits fondamentaux ainsi que des principes de nécessité et de proportionnalité. Une réforme hâtive de ces textes présenterait le risque de remettre en cause durablement certaines valeurs essentielles de notre société.

La collecte et le traitement des données afin d'assurer le suivi pourraient également présenter un important risque d'arbitraire, notamment de mésusage, d'extension d'accès ou d'élargissement des finalités, que ce soit par les pouvoirs publics ou les acteurs privés (usage policier menant à des contrôles excessifs, contrôle par l'employeur, utilisation par les assureurs, etc.). Le risque est également celui d'une défiance du public à l'égard des mesures de suivi. Ces risques nécessitent de vérifier et garantir que la collecte et le traitement des données respectent les principes de loyauté, de minimisation, de proportionnalité et de transparence, imposés en particulier par la Charte des droits fondamentaux de l'Union européenne et par le RGPD. Cela suppose encore de penser les mécanismes de gouvernance des données tels que la désignation de tiers de confiance en charge de la conception, du développement et de l'exploitation des moyens de suivi ainsi que les mécanismes de contrôle et de transparence sur le plan institutionnel, en mobilisant les autorités de régulation compétentes (CNIL, CEPD[13]) ainsi que la représentation démocratique, sous le contrôle du juge, gardien des libertés individuelles.

Le partage des données de suivi entre différents pays, sur les plans européen et international est d'un intérêt fondamental pour mieux comprendre les phénomènes observés, guider les décisions et accélérer les recherches. S'il faut donc encourager ce partage, il est important d'être attentif aux procédés de collecte, de traitement et à la maîtrise des données personnelles dans le cadre des réglementations applicables.

[12] Règlement général sur la protection des données

[13] CNIL, Commission nationale de l'informatique et des libertés et CEPD, Comité européen de la protection des données

Recommandations

- Dans la conception et la mise en œuvre des moyens de suivi, veiller à recueillir et traiter le minimum de données nécessaires au regard des finalités poursuivies et à privilégier les mesures les moins intrusives et les plus respectueuses des libertés individuelles (stockage en local, anonymisation, accès contrôlé aux données, définition des parties intervenant dans la collecte et le traitement des données, etc.).
- Garantir l'information régulière, librement accessible, loyale et transparente sur la conception, le code, l'utilisation des moyens de suivi numérique, leur finalité et l'exploitation des données collectées.
- Organiser en continu des contrôles institutionnels et démocratiques des mesures de suivi numérique et de leurs éventuelles prorogations.
- S'assurer que les échanges internationaux de données de suivi respectent le cadre européen de la protection des données et de la vie privée.

ANNEXES

AUTOSAISINE

Réflexions et points d'alerte sur les enjeux d'éthique du numérique en situation de crise sanitaire aiguë - 24 mars 2020

La crise sanitaire majeure due à la pandémie du Covid-19 accentue crucialement l'utilisation des sciences et technologies du numérique pour informer, communiquer, surveiller, recueillir et exploiter les données. Combinés à l'essor rapide du numérique ces vingt dernières années, ces usages ont des conséquences immédiates et potentiellement critiques pour les personnes, leur famille, leur activité professionnelle, leur responsabilité sociale mais aussi pour les entreprises, l'organisation du système de santé et l'organisation globale de notre pays. Il en résulte une amplification considérable des tensions entre bénéfices et risques des innovations numériques qui intervient de manière soudaine dans un contexte international lui aussi en phase critique en termes sanitaire, numérique, environnemental et économique.

Le recours au numérique dans ce contexte de crise aiguë est essentiel pour aider les soignants à comprendre et gérer la pandémie, pour les scientifiques à trouver au plus vite des stratégies thérapeutiques, médicamenteuses et vaccinales mais aussi pour l'élaboration de politiques publiques face à la crise. Il est aussi essentiel pour la continuité d'un grand nombre d'activités, professionnelles, d'éducation et de formation, d'information, de culture et de loisir, et pour la continuité du lien social. Il est source d'innovations pour comprendre et aider à gérer la crise tant au niveau sanitaire que social, économique et politique. Cependant ces usages, nouveaux ou renforcés, ne vont pas sans un accroissement de risques déjà existants et sans l'émergence de risques nouveaux. Ces risques sont liés à l'urgence des décisions à prendre, à la nouveauté de la situation, à l'impréparation en termes d'éducation ou d'organisation et à la modification des priorités entre valeurs, soulevant des questions éthiques majeures.

Différents points d'attention peuvent être d'ores et déjà identifiés, parmi lesquels : les inégalités vis- à-vis de l'usage du numérique (« fractures numériques ») ; la surveillance des personnes et la violation de l'intimité (déplacements et suivi des données de santé) ; les vulnérabilités des moyens utilisés (réseaux, applications) tant du point de vue de leur robustesse qu'en matière de sécurité, de confidentialité et de souveraineté ; la modification des liens sociaux ; la propagation des informations ou des désinformations ; et le comportement des acteurs économiques.

Dans ce contexte et dans la durée, le comité explicitera ses réflexions à destination aussi bien des citoyens que des décideurs, des médias et des responsables politiques. Il s'attachera à identifier les questions éthiques soulevées par les usages du numérique dans cette situation de crise, caractérisera les dérogations aux règles qui pourraient être autorisées pour tenir compte des impératifs de santé publique en précisant les conditions de leur mise en œuvre, tout en réfléchissant aux principes intangibles requis pour qu'en sortie de crise, le retour à une situation normale soit accompagné d'une évolution de l'usage du numérique conforme aux normes et valeurs de la société. Il signalera des points d'alerte et pourra émettre des recommandations en prenant en compte à la fois les impératifs de santé publique et le respect des droits humains fondamentaux. Cette réflexion sur les enjeux d'éthique du numérique sera complémentaire de la réflexion conduite par le CCNE sur les aspects de bioéthique face à une pandémie. Initiée et menée par nécessité dans l'urgence, elle devra se poursuivre en tenant compte des questions qui se poseront au cours de la gestion de crise jusqu'à sa fin effective.

Composition du groupe de travail

Raja Chatila
Laure Coulombel
Camille Darche
Emmanuel Didier
Karine Dognin-Sauze
Gilles Dowek
Christine Froidevaux - co-rapporteuse
Jean-Gabriel Ganascia
Eric Germain
Alexei Grinbaum
Jeany Jean-Baptiste
Claude Kirchner
Caroline Martin
Tristan Nitot
Jérôme Perrin
Catherine Tessier - co-rapporteuse
Serena Villata
Célia Zolynski

Bulletin de veille n°2 :

ENJEUX D'ÉTHIQUE DANS LA LUTTE CONTRE LA DÉSINFORMATION ET LA MÉSINFORMATION

Bulletin de veille
Publié le 21 juillet 2020

https://www.ccne-ethique.fr/fr/actualites/comite-national-pilote-dethique-du-numerique-bulletin-de-veille-ndeg2

NOTE DE SYNTHÈSE

Si le phénomène de rumeur est ancien, les développements d'internet et d'outils numériques tels que ceux mis en œuvre par les plateformes numériques – réseaux sociaux, moteurs de recherche et systèmes de partage de vidéos – lui ont conféré une ampleur sans précédent. S'appuyant sur la liberté d'expression, ces dernières se présentent en effet comme des intermédiaires techniques sans responsabilité éditoriale permettant à tous de partager un nombre considérable d'informations presque instantanément.

Durant la crise sanitaire engendrée par l'épidémie de SARS-CoV-2, l'isolement des individus en raison du confinement, l'anxiété suscitée par la gravité de la situation ou encore les incertitudes et les controverses liées au manque de connaissance sur ce nouveau virus ont exacerbé à la fois le besoin d'informations fiables et la circulation de contenus relevant de la désinformation ou de la mésinformation. Cette crise a alors conduit certaines plateformes à accentuer leur travail de modération des contenus. Or ce travail est complexe : selon le cadre dans lequel elle est présentée, la manière dont elle est formulée ou le point de vue de son destinataire, toute information est susceptible de relever finalement de la mésinformation ou de la désinformation. Par ailleurs, le fait de sélectionner, de promouvoir ou de réduire la visibilité de certaines informations échangées sur les plateformes numériques, entre en tension avec le respect des libertés d'information et d'expression.

Compte tenu de ces enjeux individuels et collectifs, le Comité national pilote d'éthique du numérique (CNPEN) s'est saisi de ce sujet dans le cadre de sa veille sur les enjeux éthiques liés aux usages du numérique en contexte de crise sanitaire[14].

Ce bulletin de veille[15] identifie tout d'abord les tensions éthiques relatives à la mise œuvre d'outils de modération et aux mécanismes de lutte contre la viralité par les plateformes à l'occasion de la crise sanitaire. Auparavant, une partie des mécanismes de lutte contre la désinformation et la mésinformation développés par ces opérateurs reposait déjà sur des outils automatisés, compte tenu du volume considérable d'informations à analyser. Durant la crise, la supervision humaine de cette détection automatisée a été réduite dès lors que les conditions de télétravail, souvent non anticipées, pouvaient amener à utiliser des réseaux non sécurisés pour transférer de tels contenus, potentiellement délictueux, ou à devoir les modérer dans un contexte privé difficilement maîtrisable. Or, les risques d'atteintes disproportionnées à la liberté d'expression se sont avérés plus importants en l'absence de médiation et de validation humaines, seules à même d'identifier voire de corriger les erreurs de classification ou les biais algorithmiques. L'emploi massif d'outils automatiques indépendamment de tout contrôle humain exercé a posteriori a en outre interrogé la possibilité de recours offerte à l'auteur d'un contenu ayant été retiré par la plateforme. Par conséquent, le comité insiste sur l'importance d'un retour rapide à une modération supervisée par des agents humains et appelle les plateformes à plus de

[14] Créé en décembre 2019 par le Premier ministre, le CNPEN a entamé un travail de veille sur les enjeux éthiques engendrés par la crise sanitaire.

[15] Son premier bulletin (https://www.ccne-ethique.fr/fr/actualites/comite-national-pilote-dethique-du-numerique-bulletin-de-veille-ndeg1) portait d'une part sur l'usage d'outils numérique dans le cadre d'actions de fraternité et sur les outils de traçage numérique d'autre part. Un autre bulletin portant sur la télémédecine est en préparation.

transparence sur les critères algorithmiques d'évaluation des informations ainsi que sur le critères retenus pour définir leur politique de modération, qu'ils soient d'ordre économique ou relèvent d'obligations légales. Il préconise également de mener une réflexion d'ampleur sur la constitution de bases de données communes pour améliorer les outils numériques de lutte contre la désinformation et la mésinformation et encourage les plateformes à partager les métadonnées associées aux données qu'elles collectent à cette fin. Enfin, il recommande que les plateformes garantissent une mise en œuvre effective des moyens techniques et humains pour lutter contre la désinformation et la mésinformation et qu'elles fassent état de leur politique de modération dans le cadre de la publication d'un rapport d'activité périodique.

Le comité relève en outre que l'ampleur prise à ce jour par les phénomènes de désinformation et de mésinformation tient à l'accroissement de la diffusion de contenus par les mécanismes de viralité qui se déploient à partir des outils offerts par les plateformes. Cela interroge tant le modèle économique de certains de ces opérateurs que le rôle joué par leurs utilisateurs dans la propagation virale de la désinformation et de la mésinformation, que ces derniers y contribuent délibérément ou par simple négligence ou ignorance. Dans cette dernière hypothèse, le comité souligne l'importance d'inciter les utilisateurs à être plus scrupuleux avant de décider de partager des informations et ainsi de contribuer à leur propagation virale. Le comité relève à cet égard que la promotion d'une conduite plus responsable suppose que les plateformes mettent à disposition de leurs utilisateurs un certain nombre d'informations et d'outils afin de les mettre en mesure de prendre conscience, voire de maîtriser, le rôle qu'ils jouent dans la chaîne de viralité de l'information. En ce sens, il recommande notamment d'indiquer explicitement qu'une information reçue a été massivement partagée et d'être vigilant avant de repartager des contenus ayant fait l'objet de signalement. Il insiste par ailleurs sur la nécessité de renforcer l'esprit critique des utilisateurs, ce qui suppose tout particulièrement que ceux-ci puissent être sensibilisés aux sciences et technologies du numérique afin de mieux maîtriser le fonctionnement de ces plateformes et les effets induits par ces mécanismes de viralité.

Si la modération des contenus et le contrôle de la viralité jouent un rôle prépondérant dans le contrôle pragmatique de la désinformation et de la mésinformation, le comité souligne que ces opérations soulèvent, dans le même temps, d'autres questionnements éthiques relatifs au rôle joué par différentes autorités dans ce processus. Il convient alors de s'interroger sur l'autorité acquise par les plateformes et d'identifier les tensions éthiques résultant des rapports que ces opérateurs entretiennent avec différentes autorités comme l'État, la justice ou la presse. À cet égard, le comité souligne la nécessité de mener une réflexion d'ensemble sur la responsabilité des plateformes ainsi que sur le contrôle à exercer s'agissant de leur politique de modération de contenus. Ce contrôle ne peut en effet être dévolu à l'État seul et devrait relever d'une autorité indépendante, incluant les représentants de diverses associations, scientifiques et acteurs de la société civile dans l'établissement des procédures de sélection d'informations à promouvoir, tout particulièrement en période de crise sanitaire.

ENJEUX D'ÉTHIQUE DANS LA LUTTE CONTRE LA DÉSINFORMATION ET LA MÉSINFORMATION

Les phénomènes de désinformation et de mésinformation ont été exacerbés à l'occasion de la crise engendrée par l'épidémie de SARS-CoV-2. Cela a conduit les plateformes numériques telles que les réseaux sociaux, moteurs de recherche, ou systèmes de partage de vidéos à développer des pratiques et des outils numériques pour contribuer à lutter contre leurs effets délétères tant sur le plan individuel que collectif.

Ce bulletin vise à identifier les tensions et enjeux éthiques résultant de ces diverses actions, ce qui nécessite de prendre en compte toute la complexité d'un tel phénomène aux implications transversales. Différentes questions peuvent alors émerger, par exemple : que traduisent ces actions ou inactions dans le contexte de la COVID-19 ? Constate-t-on simplement un changement de volume ou, plus profondément, un changement de nature des solutions numériques conçues pour lutter contre la désinformation et de la mésinformation ? Plus généralement, comment appréhender la complexité d'un tel phénomène dès lors que celui-ci appelle des analyses qui paraissent dépasser l'éthique, voire qui interrogent la notion même d'éthique ? Ainsi, la distinction entre désinformation et mésinformation engendre une tension dans la nature des prises des positions éthiques qu'on est amenés à défendre. En effet, lorsqu'il s'agit d'acteurs qui agissent en toute conscience pour tromper leur cible, la réflexion éthique tend à interroger la responsabilité de chacun ; lorsqu'elle s'adresse plutôt à ceux qui, pris dans les flux d'informations, participent à la viralité de ces informations sans en être nécessairement conscients, elle appelle surtout à une meilleure maîtrise de leur rôle dans les mécanismes de viralité de l'information numérique. En toutes hypothèses, elle nécessite d'identifier, tout particulièrement dans le cadre numérique, les dimensions économiques, juridiques, sociales, politiques ou philosophiques des mécanismes de désinformation ou de mésinformation.

Ce bulletin s'inscrit dans la lignée d'un travail de veille engagé par le CNPEN depuis le début de la crise sanitaire[16]. Il entend contribuer à cette réflexion d'ensemble sous l'angle éthique en dressant un constat des actions et inactions mises en œuvre par les plateformes à l'occasion de la crise COVID-19. À l'aune de ce contexte spécifique, il formule des recommandations et identifie plusieurs points d'attention pour nourrir une réflexion qu'il conviendra de poursuivre sur ces phénomènes de désinformation et de mésinformation à l'ère numérique.

Emmanuel Didier, Serena Villata, Célia Zolynski
Rapporteurs du groupe de travail

Claude Kirchner
Directeur du comité national pilote d'éthique du numériquea

[16] https://www.ccne-ethique.fr/fr/actualites/comite-pilote-dethique-du-numerique-bulletin-de-veille-ndeg1

INTRODUCTION

S'il a toujours existé, le phénomène de la rumeur - c'est-à-dire la diffusion au sein du public d'informations à l'origine incertaine et à la véracité douteuse - se traduit dans le monde numérique par la propagation potentiellement massive, souvent délibérée ou automatisée, d'informations de tous types. Les intentions de leurs auteurs ou de leurs propagateurs peuvent être diverses. Certaines informations sont délibérément créées pour tromper subtilement, jeter le trouble, induire en erreur des personnes, des organisations ou l'opinion publique ou encore pour favoriser certains intérêts ; le fait de diffuser ces informations avec l'intention délibérée d'induire en erreur, de causer un préjudice public, ou encore de réaliser un gain économique peut être qualifié de « désinformation ». D'autres informations peuvent s'avérer incertaines, incomplètes ou erronées alors qu'elles sont présentées comme sûres et diffusées de bonne foi par des propagateurs humains. Cela inclut tout un pan de contenus scientifiques, constitués de rumeurs, d'informations mal comprises ou mal reformulées, d'inquiétudes non fondées ou insuffisamment fondées scientifiquement, massivement diffusées par les plateformes.7 Leurs propagateurs humains n'ont généralement pas conscience des effets de cette transmission d'information, ni du fait qu'ils contribuent ainsi au modèle économique des plateformes. Cela relève alors de la « mésinformation »[17].

Produit et véhiculé sur Internet via les réseaux sociaux, les sites web, les forums ou les messageries instantanées, ce phénomène a pris une ampleur inédite depuis 2016 notamment avec la campagne de l'élection présidentielle américaine, la campagne du Brexit, et en 2017 avec la campagne présidentielle française. La crise sanitaire liée à la COVID-19 a exacerbé ce phénomène au point que les Nations Unies et plusieurs de ses agences (OMS, Unicef) évoquent désormais une véritable « infodémie »18. Confinement, isolement, anxiété, gravité de la situation ou encore multiplicité des facteurs d'incertitude constituent le terreau fertile de l'amplification de la désinformation et de la mésinformation, qui se joue tant à l'échelle individuelle que planétaire. La désinformation et la mésinformation ont ainsi pu concerner notamment l'origine et la prévention du virus SARS-CoV-2, la recherche de traitements, les conséquences de l'épidémie, les politiques de confinement et de déconfinement, l'éventuel traçage des chaînes de contamination, la discrimination de certaines populations, l'annonce de pénuries qui désorganisent sans fondement le fonctionnement de la société ou encore les publicités mensongères ou malveillantes.

---

17 Sur cette distinction, v. la Communication de la Commission européenne *Lutter contre la désinformation concernant la COVID-19 – Démêler le vrai du faux*, 10 juin 2020, JOIN(2020) 8 final, p. 4&s. CELEX 52020JC0008 FR TXT-1.pdf

18 « Les infodémies constituent une surabondance d'informations sur un problème donné, qui rend la définition d'une solution difficile. Lors d'une crise sanitaire, elles peuvent être sources de mésinformation, de désinformation et de rumeurs. Les infodémies peuvent faire obstacle à une réaction efficiente en termes de santé publique et susciter confusion et méfiance au sein de la population. » https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200305-sitrep-45-covid-19.pdf?sfvrsn=ed2ba78b_4

Cette nouvelle échelle de la désinformation est intimement associée à l'apparition des réseaux sociaux[19], moteurs de recherche[20], et systèmes de partage de vidéos[21], que nous désignons ici par le terme plateformes[22] numériques. Ces dernières augmentent significativement la capacité de leurs utilisateurs à jouir de la liberté d'expression propre à chacun, en contribuant à la diffusion, à la circulation et à l'échange d'informations. Chacun peut y exprimer son opinion librement, principe qui est revendiqué par les démocraties occidentales, ou telle est au moins la perception qu'en ont les utilisateurs. La défense de ce principe de liberté individuelle a permis aux plateformes de se présenter comme de simples diffuseurs d'informations sans responsabilité éditoriale. Or il est apparu, au moins depuis le milieu des années 2010, que cette liberté devait nécessairement être encadrée. Les scènes de violence - en particulier lorsqu'il s'agit d'actes terroristes - ou de pornographie diffusées sur les plateformes ont démontré que certains types de contenus pouvaient avoir des conséquences dangereuses pour certains groupes d'utilisateurs ou des populations entières. Des particularités culturelles font, par exemple, que la nudité fait partie de cette liste des contenus prohibés aux États-Unis d'Amérique. Dans le contexte actuel, certaines informations concernant l'épidémie, comme les publicités pour de faux remèdes, peuvent avoir des conséquences graves sur la santé. Elles peuvent aussi accentuer la défiance de la population à l'égard des autorités publiques et rendre plus difficile la gestion de la crise sanitaire. Ces effets réels et rapidement constatés ont poussé certaines plateformes à modérer davantage les contenus, voire à supprimer ou à promouvoir certaines informations.

Ce travail de modération est extrêmement complexe : toute information, quelle que soit son origine ou sa valeur de vérité, peut potentiellement devenir mésinformation ou désinformation selon le cadre dans lequel elle est présentée, la manière dont elle formulée ou le point de vue de son destinataire. En effet, l'information n'est pas seulement vraie ou fausse au sens d'une valeur de vérité ; elle est aussi inscrite dans un cours d'actions ou un contexte, dans une pragmatique, c'est-à-dire évaluée en fonction de ses sources et de ses effets avérés ou supposés. Cette évaluation comporte donc toujours une part d'incertitude et un aspect politique. Dans son actualité, l'information nécessite une mise en perspective : elle est nécessairement reçue et interprétée en fonction d'un ensemble de présupposés et d'effets sociaux et politiques propres à chaque destinataire. La valeur de vérité de l'information importe alors moins que la pragmatique de sa propagation, c'est-à-dire l'ensemble de ses conséquences et effets empiriques (à qui elle sert, comment elle permet de faire des alliances, quels types d'actions elle suscite, etc.)[23].

---

19 Facebook, Tiktok, LinkedIn, Twitter, WhatsApp, Mastodon, etc.

20 Google Chrome, Qwant, DuckDuckGo, Ecosia, etc.

21 YouTube, DailyMotion, Snapchat, etc.

22 Sur cette terminologie, v. la Communication de la Commission européenne *Lutter contre la désinformation concernant la COVID-19 – Démêler le vrai du faux,* préc. ou encore le Rapport de la mission « Régulation des réseaux sociaux – Expérimentation Facebook », https://www.vie-publique.fr/sites/default/files/rapport/pdf/194000427.pdf

23 V. également l'avis n°2018-37 du COMETS (le Comité d'éthique du CNRS) - *Quelles nouvelles responsabilités pour les chercheurs à l'heure des débats sur la post-vérité ?* 12/04/2018 : https://comite-ethique.cnrs.fr/wp-content/uploads/2019/10/AVIS-2018-37.pdf

Le problème repose alors sur l'intrication entre, d'une part, l'évaluation de la valeur de vérité des informations diffusées et, d'autre part, le degré de liberté d'expression laissé aux propagateurs relativement aux conséquences de leurs actes de parole.[24] Cette complexité de l'évaluation éthique est en outre aggravée par le fait que, sur les réseaux sociaux, tout individu ou tout groupe constitué rapidement ou spontanément (souvent uniquement en ligne) peut diffuser ses opinions à une échelle globale. Cette absence de sélection et la remise à plat des hiérarchies sociales est un facteur de premier plan dans l'analyse éthique. La situation créée par la crise Covid-19 a davantage participé à cette relativisation informationnelle : tout d'abord, le confinement a produit l'isolement des individus et les a rendus plus dépendants des réseaux numériques ; ensuite, la science, dont la temporalité est toujours plus lente que celle de l'actualité, a dû intégrer des facteurs d'incertitude radicale dans une communication sur des enjeux vitaux pour l'ensemble de la population.

Sans critère universel permettant de qualifier une information comme *fausse* puisque sa légitimité dépend de la perspective d'où elle est saisie et de la société dans laquelle elle est émise, les plateformes ont cherché à établir des cadres permettant de déterminer ce qu'il est possible ou non de diffuser. Pour cela, elles s'appuient parfois sur des associations de « *fact-checkers* », souvent organisées par les grands organes de presse, ou encore sur des autorités sanitaires ou gouvernementales nationales et internationales. Elles établissent aussi leurs propres critères permettant de discriminer des contenus jugés illicites ou dangereux des autres informations - cette détection s'appuyant souvent sur un recours massif à des outils numériques automatisés. La crise sanitaire de la Covid-19 a montré que ces ressources ne suffisaient pas : le caractère médico-scientifique des informations diffusées et des controverses dont elles pouvaient faire l'objet ont accentué la difficulté qu'il peut y avoir à identifier les autorités légitimes en matière d'information. Elle a aussi mis en évidence le fait que ces plateformes ne pouvaient définir seules de telles procédures de tri et de sélection des informations.

L'ensemble de ces phénomènes et actions, parfois amplifiés par la crise sanitaire, suscite différents questionnements de nature éthique. Il est tout d'abord nécessaire de s'interroger sur les risques potentiels d'atteintes disproportionnées aux libertés d'expression et d'information qui peuvent en résulter. Il est en effet essentiel, même en période de crise, de garantir les principes fondamentaux de nos démocraties[25] tels l'accès à l'information, la liberté d'expression, l'indépendance des médias et la délibération ouverte. Il est en outre possible d'interroger la légitimité et les effets du pouvoir, numérique et politique, qui semble ainsi acquis par les plateformes sous couvert de l'objectif de lutte contre la désinformation ou la mésinformation. L'articulation de ce pouvoir avec celui des autorités préexistantes (État, juridictions…), devrait être pensée. Plus généralement, il paraît essentiel de s'interroger sur la responsabilité éthique qui devrait incomber aux différents acteurs contribuant à la diffusion de ces contenus au moyen d'outils numériques.

[24] J.L. Austin, *Quand dire, c'est faire*, Paris, le Seuil, 1991.

[25] Sur ce point, v. la déclaration sur la liberté d'expression et d'information en temps de crise par le Comité d'experts du Conseil de l'Europe sur l'environnement des médias et la réforme (MSI-REF), 21 mars 2020 – également *Respecter la démocratie, l'état de droit et les droits de l'homme dans le cadre de la crise sanitaire du COVID-19. Une boîte à outils pour les États membres*, 7 avril 2020, SG/Inf(2020)11.

De telles interventions peuvent en effet donner lieu à des positions divergentes. On pourrait considérer que toute suppression est une atteinte à la liberté, ou bien que le dommage engendré par la suppression de certaines formes d'art ou d'humour propres aux réseaux sociaux est moindre que le dommage suscité par la diffusion de fausses informations. On pourrait également craindre que de telles pratiques induisent, par effet mimétique, le même type de censure ou d'autocensure hors des réseaux sociaux, conduisant à terme à l'appauvrissement de la vie sociale en général. Ou encore considérer que ce changement adviendra vraisemblablement, mais qu'il ne nous appartient pas d'en juger car ce sera aux générations futures de dire s'il est bon ou mauvais de leur point de vue. Il est possible de résumer la situation comme résultant des tensions entre trois éléments : premièrement, le respect de la liberté d'expression ; deuxièmement, l'identification d'autorités, nouvelles ou anciennes, ayant la légitimité de déterminer les contours de cette liberté, ainsi que les limites nécessaires au pouvoir de celles-ci ; troisièmement, les procédures concrètes de modération des échanges entre utilisateurs et plateformes traduisant en acte les décisions de ces autorités. De ce triangle de tensions émergent de nombreuses questions éthiques.

L'objectif de ce bulletin n'est pas d'évaluer la valeur de vérité de certaines informations ni les conséquences immédiates de leur diffusion ; cette tâche est celle que les acteurs du web, plateformes et autorités compétentes. Il vise à expliciter et analyser les enjeux éthiques soulevés par les choix institutionnels que les plateformes ont mis en œuvre pour lutter contre les phénomènes de désinformation et de mésinformation. Autrement dit, il ne s'agira pas d'analyser les modes de production de désinformation mais d'envisager les choix faits ou délibérément non réalisés par ces différents acteurs pour réagir au phénomène nouveau d'« infodémie » afin d'identifier les tensions éthiques que leurs actions ou inactions peuvent soulever.

Ces tensions concernent en premier lieu la mise œuvre des outils de modération et les mécanismes de lutte contre la viralité auxquels les plateformes ont recours (I) ; elles interrogent en second lieu les rapports que ces opérateurs entretiennent avec différentes autorités étatiques, judiciaires, scientifiques ainsi qu'avec la presse (II).

I. OUTILS DE MODÉRATION ET MÉCANISMES DE VIRALITÉ

Pour répondre au risque de désinformation, particulièrement accru dans le contexte de la crise COVID-19, les différentes plateformes proposent une variété de moyens pour agir sur les contenus diffusés, que ce soit pour les supprimer, réduire leur visibilité ou les promouvoir.

Suppression de contenus : La plupart des plateformes suppriment les contenus pouvant causer un danger imminent ou être préjudiciables à la santé publique (contestant, par exemple, une décision ou une recommandation d'un organisme de santé publique ou un fait scientifique) ou, plus généralement, étant susceptibles de porter atteinte à l'intégrité d'autrui ou à l'ordre public. Elles peuvent aussi refuser de diffuser les publicités identifiées comme trompeuses, mensongères ou jouant sur la panique. En temps de crise COVID-19, certaines suspendent par exemple les faux comptes d'utilisateurs se faisant passer pour des organismes de santé, ou ceux identifiés comme diffusant des informations erronées et potentiellement dangereuses pour la santé.

Réduction de la visibilité de contenus : Plusieurs plateformes réduisent la diffusion de certains contenus en les rétrogradant dans leur ordre d'apparition. Elles peuvent aussi signaler à l'utilisateur les informations douteuses et le rediriger vers des articles ou des pages de vérification des faits sur le sujet. D'autres limitent le nombre possible de transferts de contenus ou bloquent les comptes à partir desquels sont effectués des transferts en masse.

Promotion de contenus : Différentes plateformes promeuvent des informations sous la forme de bandeaux, de contenus éditorialisés ou de fils d'actualité provenant de sources qu'elles estiment de confiance tels que des organismes de santé publique, des ministères, ou des sites de vérification des faits. Elles peuvent également promouvoir ces informations en les mettant en avant dans leur référencement ou en amplifiant leur visibilité par des annonces publicitaires gratuites.

Si ces réponses, qui s'appuient sur des moyens techniques et humains, peuvent paraître *a priori* adaptées pour lutter contre la désinformation, elles posent dans le même temps différents problèmes éthiques relatifs, d'une part, à l'emploi d'outils automatiques pour détecter ce type d'informations (I.B) et, d'autre part, aux mécanismes de viralité, c'est-à-dire la diffusion rapide et imprévisible de ces contenus, qui alimentent leur propagation (I.A).

A. Les outils automatiques

Le recours à différents outils automatiques s'explique par la nécessité d'un passage à l'échelle dans la détection de contenus relevant de la désinformation ou de la mésinformation. En effet, compte tenu du nombre considérable d'informations qui circulent *via* Internet, et notamment à travers les plateformes, le recours aux outils automatiques paraît seul permettre de rendre la détection de la désinformation ou de la mésinformation plus efficace par rapport à ce que peuvent réaliser les vérificateurs humains (*fact-checkers*) en qualifiant la plupart de ces informations en très peu de temps. L'automatisation de ces procédures pose toutefois de nombreuses questions éthiques qui tiennent tant à la fiabilité de ces outils automatiques qu'à leurs effets s'agissant du respect de la liberté d'expression.

Tout d'abord, lorsqu'ils sont totalement automatisés, ces outils peuvent comporter des biais algorithmiques ou des erreurs de classification. Quant à leur fonctionnement, ces outils utilisent divers algorithmes de détection automatique de la désinformation ou de la mésinformation adaptés à différents supports (texte, vidéos, images). Ces algorithmes se fondent notamment sur la reconnaissance de mots clés dans les textes, la détection de la réutilisation d'images anciennes à travers l'analyse de la chronologie ou encore la détection de l'angle du visage, de son teint et de son expression, l'éclairage et d'autres informations importantes pour vérifier l'authenticité de vidéos de personnes.

.

Pour aller plus loin

Évaluer la véracité d'une information est une tâche complexe et lourde, même pour des experts qualifiés tels que les fact-checkers *humains[1]. Par exemple, une première étape pour identifier les contenus relevant de la désinformation ou de la mésinformation consiste à analyser ce que les autres sources d'information disent sur le sujet. Cette tâche automatique est appelée "*stance detection*" et consiste à estimer la position relative de deux morceaux de texte par rapport à un sujet. Cette approche permet d'établir la cohérence de ces contenus (*consistency*).*

Il existe différentes stratégies d'étiquetage ou de classement pour la détection des contenus relevant de la désinformation ou de la mésinformation. Dans la plupart des études, la détection de ces informations est formulée comme un problème de classification ou de régression. L'approche la plus courante consiste à formuler la tâche de détection de ces informations comme un problème de classification binaire (désinformation ou non). Cependant, classer tous ces contenus en deux classes est difficile parce qu'il y a des cas où les contenus ne relèvent que partiellement de la désinformation (seulement une portion du contenu relève de la désinformation ou de la mésinformation). La détection de ces informations peut également être formulée comme une tâche de régression, où le résultat est un score numérique de véracité.

Ces approches algorithmiques de détection automatique de la désinformation ou de la mésinformation sont confrontés à plusieurs défis. Un premier défi important est lié à la disponibilité et la qualité des données : pour que les classificateurs atteignent de bonnes performances, ils doivent disposer de suffisamment de données étiquetées. Or l'étiquetage fiable d'un large volume de données implique un travail long et complexe de la part d'experts qualifiés. La détection du contexte représente un autre défi important. Elle suppose de mettre au point des algorithmes en mesure d'analyser efficacement des informations à long terme et de transition de contenu en utilisant des connaissances de base. Enfin, un troisième défi consiste dans le croisement des données multimodales. En effet, pour être détectés efficacement, certains contenus supposent de croiser différents types d'informations tels que du texte, des images et les métadonnées associées à ces contenus

Compte tenu de ces difficultés, l'automatisation de la détection de contenus relevant de la désinformation ou de la mésinformation peut conduire à un certain nombre d'erreurs de classification, appelées faux positifs, c'est-à-dire d'informations classifiées à tort comme relevant de la désinformation ou de la mésinformation. Cela concerne notamment les contenus humoristiques, ironiques ou caricaturaux, ou encore les informations nécessitant la prise en compte de diverses connaissances antérieures pour permettre une classification appropriée. Cette détection automatique peut aussi être source de faux négatifs : des informations relevant bien de la désinformation ou de la mésinformation peuvent ne pas être pas détectées par l'algorithme et continuer à être diffusées sur les plateformes. De plus, d'éventuels biais algorithmiques de fonctionnement peuvent influencer la détection de la désinformation ou de la mésinformation. Ces biais sont dus à des choix conscients ou inconscients des développeurs ou à des biais provenant des données et peuvent entraîner une discrimination indirecte d'une partie des utilisateurs.

Bien qu'elle soit rendue nécessaire par le volume considérable d'informations à analyser, cette vérification algorithmique peut donc induire des risques de censure et d'atteintes disproportionnées à la liberté d'expression. Ces risques de biais algorithmiques et d'erreur de classification sont d'autant plus importants en l'absence de mécanismes de médiation et de validation finale par un être humain. Or, à l'occasion de la crise sanitaire, il est apparu que les plateformes n'ont pas été en mesure de laisser leurs équipes de modérateurs, en situation de télétravail, accéder à toutes les informations nécessaires du fait de leur contenu potentiellement intrusif ou dérangeant (contenus violents, propos haineux, …). En effet, les conditions de télétravail, souvent non anticipées, pouvaient amener à utiliser des réseaux non sécurisés pour transférer de tels contenus (potentiellement délictueux) ou à devoir les modérer dans un contexte privé difficilement maîtrisable. Cela a donc engendré un moindre contrôle humain de ces processus de suppression, réduction ou promotion de contenus, alors que la désinformation et la mésinformation progressaient fortement. Par ailleurs, l'emploi massif d'outils automatiques indépendamment de tout contrôle humain exercé *a posteriori*, qui peut induire un risque de censure automatique, interroge la possibilité de recours offert à l'auteur d'un contenu ayant été retiré par la plateforme.

Ensuite, le recours massif aux outils automatiques interroge la transparence et l'explicabilité des algorithmes mis en place pour détecter la désinformation ou la mésinformation. Cette problématique recouvre deux aspects distincts. D'une part, elle est relative à l'explication du résultat produit par l'algorithme et les principaux éléments pris en compte pour y parvenir (ex. les caractéristiques utilisées par le système de classification supervisé pour discriminer les contenus relevant de la désinformation, le degré de fiabilité estimé par l'algorithme du résultat obtenu, les données d'apprentissage les plus influentes pour la tâche de classification, les caractéristiques d'entrée les plus marquantes ou les caractéristiques significatives à l'intérieur des couches d'un réseau de neurones). D'autre part, le manque de transparence concerne aussi les critères retenus par les plateformes pour définir leur politique de modération (qu'ils soient d'ordre économique ou qu'ils relèvent d'obligations légales, etc.). Les solutions algorithmiques mises en place dans ces outils peuvent ainsi induire des biais "de décision" (ou volontaires) qui influencent la modération de contenus. La question se pose alors de savoir si la plateforme doit être

transparente sur ces différents critères à l'égard de ses utilisateurs et des régulateurs, dans le prolongement des obligations qui lui sont imposées par la loi du 22 décembre 2018 s'agissant de la lutte contre la mésinformation en période électorale[26].

Recommandations :

1.1 Garantir, y compris après la crise, l'existence d'une modération par l'humain permettant de vérifier les résultats produits automatiquement par les algorithmes d'analyse de contenus.

1.2 Maintenir, y compris au cours de la crise, les instruments de recours ouverts à l'auteur d'un contenu s'agissant des décisions de suppression ou promotion de contenus prises par la plateforme sur la base d'un traitement algorithmique.

1.3 Promouvoir la transparence et l'explicabilité, et donc l'« auditabilité » des algorithmes de détection de désinformation ou mésinformation et de recommandation de contenus utilisés par les plateformes, plus encore en période de crise. Exposer aux utilisateurs les critères qui fondent la décision algorithmique afin de protéger la liberté d'expression face aux trois réponses proposées par les plateformes : suppression de contenus, réduction de la visibilité de contenus, promotion de contenus.

Un autre problème tient encore à l'inégalité de performance dans la tâche de détection automatique des contenus relevant de la désinformation ou de la mésinformation entre la recherche publique et les plateformes en raison d'un accès très limité aux données de ces dernières. Ces données sont d'une grande utilité, tant pour les vérificateurs humains que pour l'amélioration des algorithmes automatiques. Les annotations visant à identifier le type de désinformation ou de la mésinformation (par exemple une citation tronquée), les méta-informations telles que la source, la date et l'heure de publication ou encore les partages de ce contenu sur Internet peuvent en effet contribuer à améliorer ces algorithmes de détection. Cela interroge alors la gouvernance de l'ensemble des données liées à la désinformation ou à la mésinformation identifiées et collectées par les plateformes et sur l'utilité qu'il y aurait à favoriser le partage de ces données entre

[26] Loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information, art. 11. V. également la recommandation du CSA n° 2019-03 du 15 mai 2019 : "le Conseil encourage les plateformes à assurer à chaque utilisateur :
- la traçabilité de ses données exploitées à des fins de recommandation et de hiérarchisation des contenus, qu'elles soient fournies sciemment ou collectées par l'opérateur de la plateforme en ligne ;
- une information claire, suffisamment précise et facilement accessible sur les critères ayant conduit à l'ordonnancement du contenu qui lui est proposé et le classement de ces critères selon leur poids dans l'algorithme ;
- une information claire et précise sur sa faculté, si elle existe, de procéder à des réglages lui permettant de personnaliser le référencement et la recommandation des contenus ;
- une information claire et suffisamment précise sur les principaux changements opérés dans les algorithmes de référencement et de recommandation, ainsi que sur leurs effets ;
- un outil de communication accessible permettant l'interaction en temps réel entre lui et l'opérateur, et offrant à l'utilisateur la possibilité d'obtenir des informations personnalisées et précises sur le fonctionnement des algorithmes".
V. également, s'agissant des relations entre plateformes et utilisateurs consommateurs, les obligations imposées aux opérateurs au titre des articles L. 11-7 &s. du Code de la consommation.

différents acteurs[27]. La question se pose tout particulièrement lorsque l'État, comme en période de crise COVID-19, entend associer les plateformes à une politique publique de lutte contre la désinformation. Il conviendrait par exemple de mettre au point des mécanismes de partage mieux adaptés et synchronisés à l'échelle continentale ou internationale, tout en offrant aux scientifiques, aux citoyens, et à la société civile la possibilité de contribuer à leur développement et mise à jour.

<u>Point d'attention :</u>

1.a Comme le préconise le rapport de la mission « Régulation des réseaux sociaux – Expérimentation Facebook »[28] et la Commission Européenne[29], il convient d'encourager à ce que soit menée une réflexion d'ampleur sur la constitution de bases de données communes pour améliorer les outils numériques de lutte contre la désinformation et la mésinformation et d'inciter les plateformes à partager les métadonnées associées aux données qu'elles collectent à cette fin (ex. source, sujet, citations, partages sur les plateformes, contre-arguments publiés en tant que commentaire de ces contenus). De telles bases de données permettraient en outre de faciliter la recherche scientifique dans ce domaine.

Au-delà, se pose également la question de la mise en œuvre effective de ces moyens techniques et humains par les plateformes pour lutter contre la désinformation et la mésinformation. Il a pu être notamment constaté une ambiguïté dans l'attitude de certaines plateformes qui, en dépit des annonces faites sur les actions menées pour lutter contre la désinformation sur les enjeux de la crise COVID-19, laissaient leurs outils publicitaires à la disposition de certains sites qui en étaient à la source[30]. S'agissant de la lutte contre la haine en ligne, la loi visant à lutter contre les contenus haineux sur internet entendait y remédier en imposant aux plateformes de rendre compte au CSA des moyens matériels et humains qu'elles mettent en œuvre pour lutter contre la diffusion de contenus visés par la liste des infractions définies par le texte[31]. La loi du 22 décembre 2018, qui impose aux plateformes de prendre des mesures en vue de lutter contre la diffusion de fausses informations susceptibles de troubler l'ordre public ou d'altérer la sincérité d'un

---

[27] V. l'article 7-III de la loi visant à lutter contre les contenus haineux sur internet (version votée par Parlement mais jugée contraire à la Constitution par la décision du Conseil constitutionnel n°2020-801 DC du 18 juin 2020) encourageant les plateformes, sous l'égide du CSA, à mettre en œuvre des outils de coopération et de partage d'informations, dans un format ouvert entre ces opérateurs, dans la lutte contre les infractions visées par le texte (contenus haineux).

[28] Rapport de la mission « Régulation des réseaux sociaux – Expérimentation Facebook » – https://www.vie-publique.fr/sites/default/files/rapport/pdf/194000427.pdf, p. 18.

[29] A ce titre, v. la Communication "Lutter contre la désinformation concernant la COVID-19 – Démêler le vrai du faux" préc., section 5.2.

[30] Sur ce point, v. notamment le rapport de l'ONG Tech Transparency Project : https://www.techtransparencyproject.org/articles/google-profiting-coronavirus-conspiracy-sites

[31] Loi visant à lutter contre les contenus haineux sur internet, article 5 jugé contraire à la Constitution par la décision du Conseil constitutionnel préc. S'agissant des critiques adressées face à l'inaction de certaines plateformes, v. par ex. l'action intentée par quatre associations (Union des étudiants juifs de France (UEJF), J'accuse, SOS-Racisme et SOS-Homophobie) contre Twitter : https://www.lemonde.fr/pixels/article/2020/05/12/twitter-assigne-en-justice-pour-son-inaction-massive-face-aux-messages-haineux_6039412_4408996.html

des scrutins, précise que ces mesures et leurs modalités de mise en œuvre doivent être rendues publiques[32]. Par ailleurs, la Commission européenne a annoncé en juin 2020 qu'il serait demandé aux plateformes de remettre un rapport mensuel sur leurs politiques et actions visant à lutter contre la désinformation liée à la COVID-19 précisant notamment les données sur les flux de publicité liés à la désinformation. Les autorités de contrôle et leurs utilisateurs pourront ainsi en évaluer l'efficacité ainsi que la réalité des promesses faites par les opérateurs[33].

Recommandation :

1.4 Mettre en place les mécanismes permettant de s'assurer que les plateformes diffusent un rapport d'activité périodique, accessible aux autorités de contrôle ainsi qu'à leurs utilisateurs, exposant de façon claire, loyale, précise et transparente leur politique de gestion de lutte contre la désinformation et la mésinformation, les moyens matériels et humains mis en œuvre à cette fin et les données relatives aux flux de publicité liés à la désinformation.

Point d'attention :

1.b Une réflexion d'ampleur devrait être menée à l'avenir sur les ressources à allouer à la modération humaine et la répartition des coûts en résultant, la qualification des modérateurs humains, le traitement des biais culturels éventuels voire les critères sur lesquels ils fondent leur décision et leur éventuel contrôle par une autorité indépendante, notamment le juge comme garant des libertés fondamentales.

B. Les mécanismes de viralité

L'ampleur prise à ce jour par les phénomènes de désinformation et de mésinformation tient à l'accroissement de la diffusion de ces contenus par les mécanismes de viralité qui se déploient à partir des outils offerts par les plateformes et les moteurs de recherche. Leur modèle économique peut amplifier un tel phénomène dès lors qu'il repose sur l'économie de l'attention qui encourage la viralité, source de bénéfices (I.2.a). Les utilisateurs jouent également un rôle dans ce phénomène puisque les micro-actions (réexpédier, partager, etc.) en sont le déclencheur initial (I.2.b).

a. Modèle économique des plateformes favorisant la viralité

Le modèle économique de certaines plateformes est fondé sur la rémunération au nombre de clics - donc sur la promotion des Clickbaits (« pièges à clics ») - et repose sur la captation et la valorisation de l'attention de leurs utilisateurs auprès des annonceurs. Ce modèle s'appuie sur un système algorithmique de priorisation des contenus qui met en avant les

[32] Loi n°2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information, article 11.

[33] En ce sens, v. les propositions faites par la Commission européenne dans sa Communication du 10 juin 2020 préc., p. 10-11.

contenus suscitant le plus de réactions et de conversations. Ainsi, il participe grandement aux mécanismes de viralité. Un tel fonctionnement peut produire des effets délétères : il conduit à faire primer des contenus concentrant davantage l'attention par des effets de coordination virale (souvent des contenus choquants, haineux ou des fausses nouvelles)34, par rapport aux contenus publiés par la presse. Ces informations sont alors souvent placées au second rang35, afin d'offrir plus de visibilité aux contenus viraux qui génèrent davantage de revenus publicitaires. Cet « engagement métrique », qui a pour objectif principal la captation, la rétention et la monétisation de l'attention des utilisateurs des plateformes, est formalisé dans le code sous une forme algorithmique, ce qui accentue le risque de promotion de fausses nouvelles si elles sont attrayantes. Ce modèle paraît en outre conduire à une forme d'hyper personnalisation des contenus qui enferme les internautes dans des bulles filtrantes et amplifie leurs biais sociologiques et cognitifs, en particulier l'homophilie - tendance à former des liens avec des individus qui nous ressemblent - et le biais de confirmation - tendance à privilégier les informations confirmant nos hypothèses36. Les actions mises en œuvre par les plateformes pour accompagner la lutte contre la crise Covid-19 ne doivent pas occulter les limites de ces modèles économiques.

<u>Point d'attention :</u>

1.c Il sera souhaitable d'approfondir l'analyse des mécanismes sur lesquels reposent les marchés de publicité en ligne dont les ressorts et les critères de fixation des prix sont pour l'heure opaques et soulèvent un certain nombre d'enjeux éthiques.

b. Viralité et rôle des utilisateurs

Si les plateformes jouent bien un rôle d'amplificateur dans la diffusion des contenus, il convient d'analyser les différentes causes des mécanismes de viralité et, en particulier, le rôle d'utilisateurs individuels ou de groupes d'utilisateurs dans ce mécanisme[37].

Le rôle des utilisateurs se joue en effet à deux niveaux : d'une part, en leur qualité de destinataires de l'information, d'autre part, en leur qualité d'agents de la viralité dès lors qu'ils participent à la propagation des informations en publiant, republiant et commentant différents contenus textuels ou visuels (mème, GIF, etc.). A ce titre, il faut distinguer deux types d'utilisateurs – sachant qu'un individu ou un groupe peut passer d'un type à l'autre en fonction des circonstances. D'une part, on trouve ceux qui participent intentionnellement à cette propagation, la plupart du temps pour des motifs idéologiques ou cupides. Ce type de comportements pose la question de la responsabilité et des

---

34 D. Cardon, *A quoi rêvent les algorithmes. Nos vies à l'heure des big data,* Seuil, 2015, p. 91.

35 B. Patino, *La civilisation du poisson rouge. Petit traité sur le marché de l'attention*, Grasset, 2019, p. 141.

36 Ce dernier phénomène est toutefois discuté : v. not. F. Tarrisan, *Au coeur des réseaux*, Le Pommier, 2019, p. 115 &s.

37 En ce sens, v. le rapport visant à renforcer la lutte contre le racisme et l'antisémitisme sur Internet, remis au Premier ministre en septembre 2018 par L. Avia, K. Amellal et G. Taieb, https://www.gouvernement.fr/sites/default/files/contenu/piece-jointe/2018/09/rapport_visant_a_renforcer_la_lutte_contre_le_racisme_et_lantisemitisme_sur_internet_-_20.09.18.pdf, pt. 6.1.

sanctions applicables à de tels comportements sur le plan juridique. D'autre part, on trouve les acteurs qui peuvent participer à la viralité par simple négligence ou ignorance des effets néfastes que celle-ci peut engendrer.

Il paraît nécessaire d'inciter ces derniers à être scrupuleux avant de décider de partager des informations et ainsi de contribuer à leur propagation virale. Si ce partage relève, sur le plan éthique, de leur responsabilité en tant qu'acteurs de la diffusion d'une information douteuse ou erronée, la promotion d'une conduite plus responsable suppose que les plateformes mettent ces utilisateurs en mesure de prendre conscience, voire de maîtriser, le rôle qu'ils jouent dans la chaîne de viralité de l'information. A ce titre, la loi du 22 décembre 2018 sur la lutte contre la mésinformation impose aux plateformes de mettre en place des dispositifs appropriés permettant aux utilisateurs d'être informés sur la nature, l'origine et les modalités de diffusion des contenus. Le CSA[38] recommande ainsi aux opérateurs de plateforme en ligne de veiller à :

- distinguer clairement les contenus sponsorisés des autres contenus et encourager le développement d'outils permettant à l'utilisateur d'identifier les critères qui ont conduit la plateforme à lui proposer de tels contenus ;
- appeler les utilisateurs à faire preuve de vigilance concernant les contenus qui ont fait l'objet de signalements[39] ;
- identifier de façon claire l'origine des contenus diffusés et l'afficher de manière visible ;
- préciser les modalités de diffusion des contenus en indiquant dans la mesure du possible les conditions de leur publication telles que l'existence de contreparties financières, l'ampleur de la diffusion (nombre de vues, type de population ciblée, etc.), et s'ils ont été générés de manière automatisée ou non.

Afin de permettre à l'utilisateur de mesurer et maîtriser son rôle dans la chaîne de viralité, il s'agirait par ailleurs de demander aux plateformes d'offrir à leurs utilisateurs la possibilité de :

- mesurer, lorsqu'ils utilisent un réseau social, la tribune qu'ils offrent aux contenus qu'ils diffusent directement (par publication sur son propre profil ou par "retweet" ou "share") ou indirectement (par "like") ;
- réaliser que les informations qu'ils diffusent ou relaient sont autant d'indications permettant notamment aux réseaux sociaux de les profiler plus précisément.

[38] Recommandation du CSA n° 2019-03 du 15 mai 2019 aux opérateurs de plateforme en ligne dans le cadre du devoir de coopération en matière de lutte contre la diffusion de fausses informations, n°5.
[39] Par exemple, le « flaggage » de fausses nouvelles par les plateformes.

Recommandations aux plateformes :

1.5 Mettre en œuvre les recommandations formulées par le CSA concernant la mise en place de dispositifs appropriés permettant aux utilisateurs d'être informés sur la nature, l'origine et les modalités de diffusion des contenus, et tout particulièrement demander aux plateformes :

- d'indiquer explicitement à leurs utilisateurs qu'une information reçue a été massivement partagée ;
- d'être vigilant avant de repartager des contenus ayant fait l'objet de signalement

1.6 Développer et mettre à disposition les outils permettant à leurs utilisateurs de prendre conscience de la tribune qu'ils offrent aux contenus qu'ils diffusent, directement ou indirectement, par l'intermédiaire de la plateforme.

Points d'attention :

1.d S'il est important, comme le souligne le CSA, de promouvoir les outils permettant à l'utilisateur d'identifier les critères qui ont conduit la plateforme à lui proposer de tels contenus (comprendre ce qu'il voit), un autre enjeu éthique conduira à développer les outils permettant d'assurer aux utilisateurs la capacité de préciser les critères de mise en visibilité de certains contenus à leur égard, pour tenir compte de leurs propres intérêts.

1.e Par ailleurs, et compte tenu du volume et de la vitesse de propagation de l'information circulant sur les plateformes, en particulier sur les réseaux sociaux, une réflexion pourrait être menée sur l'utilité de penser le ralentissement d'une telle circulation par le recours à des moyens numériques. Il s'agirait ainsi de rendre l'utilisateur plus scrupuleux et de l'inciter à analyser d'avantage son contenu lorsqu'il entend partager une information de façon spontanée.

Plus généralement, il conviendrait de favoriser le développement de l'esprit critique des utilisateurs afin qu'ils soient en mesure de partager un contenu en connaissance de cause. Les plateformes pourraient ainsi rappeler aux utilisateurs l'intérêt d'évaluer la pertinence et la fiabilité de leurs sources, par exemple en comparant une information aux autres informations dont ils disposent, et en menant une recherche, même brève, sur les sources et les analyses relatives à cette information.

Il s'agirait de l'inviter notamment à :

1.f chercher à identifier la source de l'information, s'interroger sur la confiance qu'on peut lui accorder, vérifier son référencement et croiser différentes sources sur le même sujet.

1.g tenir compte, avant de la partager, du caractère potentiellement incertain d'une information en particulier dans un contexte de crise sanitaire où beaucoup d'inconnues subsistent[40].

Renforcer l'esprit critique de l'utilisateur supposerait surtout de développer sa culture numérique tant sur le plan scientifique[41] que s'agissant du fonctionnement des outils numériques. A cette fin, de nouvelles ressources innovantes ont été développées par divers acteurs en lien avec la crise sanitaire, qui devraient être complétées par des actions à plus long terme[42].

Par ailleurs, une formation aux outils numériques devrait être apportée aux publics les plus vulnérables, en particulier les plus jeunes et les plus âgés, mais également être assurée tout au long de la vie[43]. A ce titre, une attention toute particulière devrait être portée à la compréhension des interfaces utilisées par les plateformes pour identifier une information erronée et permettre aux utilisateurs d'associer la bonne sémantique aux symboles utilisés. L'État pourrait ainsi lancer des campagnes d'éducation à large échelle. Il conviendrait également d'impliquer les plateformes dans ce processus de formation de l'ensemble de leurs utilisateurs.

Recommandation à l'État et aux plateformes :

1.7 Diffuser une infographie claire et accessible à tous détaillant les étapes de la réflexion à mener concernant la qualité de l'information avant de la repartager.

Points d'attention :

1.h La crise COVID-19 a confirmé l'importance de sensibiliser et d'éduquer l'ensemble des citoyens sur les enjeux de la désinformation et de la mésinformation, particulièrement amplifiée par l'usage d'outils numériques. Il convient par conséquent de mener une réflexion d'ampleur sur le sujet.

1.i Il semble particulièrement important de concevoir des campagnes de formation relatives aux outils numériques, dans le cadre de la formation initiale et tout au long de la vie, y compris pour les plus âgés. Ces formations doivent permettre aux utilisateurs de mieux évaluer la qualité des sources d'information et de maîtriser leur rôle viral.

---

40 À ce titre, v. par exemple l'infographie diffusée par *Infographie International Federation of Library Association and Institutions (IFLA)* : french_-_how_to_spot_fake_news_0.pdf

41 Dans sa résolution du 21 février 2017, sur les sciences et le progrès dans la République, l'Assemblée nationale plaide pour que « la culture scientifique soit le ferment indispensable pour des citoyens éclairés et responsables ».

42 Par exemple, l'AMCSTI (réseau professionnel des cultures scientifiques, techniques et industrielles – www.amcsti.fr).

43 En ce sens, v. CNCDH, Avis relatif à la proposition de loi visant à lutter contre les contenus haineux sur internet, 9 juil. 2019, p. 8 : final_avis_relatif_a_la_ppl_lutte_contre_la_haine_en_ligne.pdf. V. également la Recommandation du CSA n° 2019-03 du 15 mai 2019 préc., n°6.

II. LE RÔLE DES AUTORITÉS

Si la modération des contenus et le contrôle de la viralité jouent un rôle prépondérant dans le contrôle pragmatique de la désinformation et de la mésinformation, ces opérations soulèvent d'autres questionnements éthiques relatifs au rôle joué par différentes autorités dans ce processus. Cela interroge tout d'abord l'autorité ainsi acquise par les plateformes et le contrôle qui devrait en résulter (2.1). Ensuite, il apparaît que ces opérations ne peuvent se passer d'instances qui identifient les informations recevables et celles qui ne le sont pas. Différentes questions émergent alors s'agissant de la légitimité dont jouissent ces instances dès lors qu'elles sont considérées par les plateformes comme contribuant à établir, *hic et nunc*, la vérité (2.2).

A. L'autorité acquise par les plateformes

Premières responsables de l'identification de désinformation ou de mésinformation et des réponses à y apporter, les plateformes acquièrent une très grande autorité sur le partage d'information. Or leurs pratiques habituelles de modération ont été en partie transformées par la crise COVID-19 (voir supra). Différents niveaux de questionnement peuvent en résulter.

Les multiples mesures mises en œuvre par les plateformes dans le cadre de la lutte contre la crise sanitaire (suppression, réduction de visibilité et promotion de contenus) interrogent ainsi l'évolution possible de leur fonction d'intermédiaire technique. En effet, ces mesures remettent largement en cause la position longtemps défendue par ces plateformes consistant à dire qu'en tant que simples diffuseurs de contenus sans rôle éditorial, elles n'auraient pas à intervenir sur ce qui est publié par leurs abonnés, permettant ainsi à tout un chacun d'exprimer ses idées sans sélection. Mais cet argument a commencé à être battu en brèche à la suite de la vague d'actes terroristes des dernières années. Par l'appel de Christchurch, en mai 2019, ces entreprises se sont en effet engagées à ne pas diffuser sur leurs plateformes des contenus à caractère terroriste. Cette évolution est confirmée par la crise sanitaire de la COVID-19. La mise en visibilité et l'affichage de certains contenus ont en effet atteint des proportions jamais atteintes auparavant. L'accentuation de ces pratiques éditoriales peut avoir plusieurs conséquences. Par exemple, si des choix éditoriaux, comme la promotion d'informations officielles ne sont pas rendus visibles pour l'utilisateur, la neutralité des moteurs de recherche pourrait être remise en question.

<u>Recommandation aux plateformes :</u>

2.1 Indiquer clairement à leurs utilisateurs que certaines propositions d'information résultent de choix éditoriaux, qui peuvent changer en temps de crise.

Plus généralement, l'autorité que peuvent exercer les plateformes lorsqu'elles définissent leur politique de modération de contenus peut faire l'objet de diverses tensions éthiques.

On peut considérer que chaque plateforme doit être en mesure d'agir comme elle l'entend, sous réserve de se conformer à ses obligations légales. Cela peut alors les conduire à prendre des positionnements différents, conformément à leurs propres intérêts économiques et politiques, tout en arguant du rôle qu'elles pourraient jouer en tant que gardienne de la démocratie ou de la liberté d'expression de leurs utilisateurs (voir les différences de traitement des messages du président Trump par Facebook et Twitter pendant l'actuelle campagne présidentielle). En ce sens, on rappellera que ces opérateurs économiques ne sont pas qualifiés de média et ne sont donc pas soumis à une obligation de pluralisme ; ils se distinguent également des opérateurs de communication électroniques qui se voient imposer une obligation de neutralité dans l'acheminement des contenus[44].

On peut encore considérer que certaines plateformes – comme les grands réseaux sociaux – constituent de nouvelles agoras numériques, des lieux de l'expression publique. De plus, ces agoras voient l'interaction d'un nombre croissant de *bots* (utilisateurs artificiels) ayant un grand pouvoir de persuasion à travers les contenus qu'ils génèrent et font, pour certains d'entre eux, courir le risque de diffuser massivement des contenus pouvant avoir des finalités de déstabilisation économique et politique. Ceci pourrait commander une révision de leur statut, d'autant plus lorsque ces plateformes deviennent l'un des instruments d'une politique de santé publique comme en période de crise COVID-19.

On peut également interroger la légitimité des plateformes à évaluer la licéité d'un contenu, et à décider seules de son éventuel retrait, dès lors que cela revient à consacrer une forme de justice privée et à accroître des phénomènes de censure constituant autant d'atteintes à la liberté d'expression. Cela conduit alors à penser le rôle du juge qui, en sa qualité de garant des libertés fondamentales, ne saurait être relégué au second plan. Mais cela impose alors d'évaluer l'effectivité de son contrôle compte tenu de la masse des contenus visés et de leur vitesse de propagation, ou encore eu égard à sa portée territoriale potentiellement limitée alors que la plupart des plateformes opèrent à échelle mondiale et ne se limitent pas à un territoire national.

Par ailleurs la responsabilité de ces opérateurs peut être interrogée, tant lorsqu'ils procèdent à ce type de choix éditoriaux que lorsqu'ils contribuent, par défaut, à la propagation de désinformation et de mésinformation[45]. Cette responsabilité est actuellement limitée dès lors qu'ils bénéficient de la qualification d'hébergeur au sens de la loi n° 2004-575 du 21 juin 2004 pour la confiance de l'économie numérique transposant la directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 sur le commerce électronique. Différentes discussions sur une redéfinition possible de la responsabilité de ces plateformes sont d'ailleurs engagées, en Europe[46] et aux États-Unis[47]. Quoiqu'il en soit, leur responsabilité en cas de retrait ou de non retrait de contenus devrait alors être pensée dans le respect de liberté d'expression, ce que rappelle la récente

---

44 Sur ce point, v. l'étude annuelle du Conseil d'État, Numérique et droits fondamentaux, 2014, p. 217&s.

45 En ce sens, Créer un cadre français de responsabilisation des réseaux sociaux, rapport préc.

46 A cet égard, v. la consultation en cours sur la future législation sur les services numériques : https://ec.europa.eu/commission/presscorner/detail/fr/ip_20_962

47 https://www.lemonde.fr/pixels/article/2020/05/28/dans-sa-charge-contre-twitter-donald-trump-veut-changer-le-regime-de-responsabilite-des-reseaux-sociaux_6041052_4408996.html

censure par le Conseil constitutionnel de la loi visant à lutter contre les contenus haineux sur internet[48].

Point d'attention :

2.a Promouvoir la réflexion sur la redéfinition de la responsabilité des plateformes aux niveaux national et européen dans le respect de la protection de la liberté d'expression.

Une autre difficulté porte sur le contrôle de ces nouvelles autorités. La question n'est certes pas nouvelle mais pourrait se reposer à l'aune de l'accroissement du rôle joué par les plateformes dans le traitement de l'information à l'occasion de la crise Covid-19. L'Union européenne se montrait jusqu'alors plutôt favorable à une autorégulation également promue par les plateformes (v. la promotion des guides de bonne conduite[49]) alors que certains États, à l'image de la France, ont préféré instituer un contrôle par l'autorité publique (v. s'agissant de la désinformation, la loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information). D'autres encore proposent que ce contrôle soit exercé par des autorités indépendantes à la fois des plateformes et de l'autorité publique[50]. L'existence d'un tel contrôle soulève de nombreux questionnements éthiques. Il conviendrait alors de prendre en compte les bénéfices et les risques soulevés par des actions de contrôle, notamment en matière de liberté d'expression ainsi que les limites à ne pas dépasser. Il faudrait en outre évaluer les effets et les limites de l'autorégulation des plateformes s'agissant de la lutte contre la désinformation et la mésinformation et se demander si une éthique inspirée de la déontologie journalistique pourrait être appliquée aux réseaux sociaux. Il serait nécessaire de penser de nouvelles formes de régulation, notamment par une autorité indépendante, bien que son rôle puisse être délicat.

Points d'attention :

2.b Mener une réflexion d'ensemble sur le contrôle des plateformes et en particulier sur la consécration d'une nouvelle autorité chargée de leur régulation, ou sur le renforcement du rôle d'une autorité indépendante existante en charge de leur régulation comme le CSA qui pourrait devenir un Conseil supérieur de l'audiovisuel et du numérique.

2.c Permettre aux utilisateurs et à la société civile de s'organiser pour s'imposer comme un interlocuteur à part entière de ces plateformes numériques dans un souci d'autonomie et de responsabilisation de tous les acteurs, citoyens, associations, entreprises aux côtés des institutions démocratiques.

---

48 Conseil constitutionnel, Décision 2020-801 DC du 18 juin 2020, préc.

49 Lutter contre la désinformation en ligne : une approche européenne, Communication de la Commission européenne COM(2018) 236 final, 26 avril 2018

50 En ce sens, v. notamment le rapport Créer un cadre français de responsabilisation des réseaux sociaux : agir en France avec une ambition européenne, préc., quatrième pilier.

B. Les autorités sur lesquelles s'appuient les plateformes

Afin de contrôler et vérifier les informations circulant sur Internet, en particulier en cas de crise sanitaire, les plateformes numériques doivent pouvoir les comparer à des informations émanant de sources considérées étant sûres ou légitimes : "vérificateurs de faits", les services gouvernementaux, et le Service statistique public qui fournit l'immense majorité des chiffres concernant la pandémie. Or les rapports avec ces instances peuvent, eux-aussi, être source d'un certain nombre de difficultés.

Pour mieux discriminer les informations faisant autorité des autres, les plateformes peuvent par exemple s'appuyer sur le travail des vérificateurs de faits (« *fact checkers* »). Différents acteurs s'organisent au niveau national à l'image, en France, des Décodeurs du Monde, *Checknews* de Libération, *Fake off* de 20 minutes ou Factuel de l'AFP. Des associations internationales voient également le jour comme le *European Digital Media Observatory* (EDMO), soutenu par l'Union Européenne[51]. Il s'agit souvent d'émanations d'organes de presse, d'universitaires, ou d'acteurs de la société civile. Ces acteurs enquêtent sur des contenus viraux et tentent d'évaluer leur degré de véracité. Pour cela, ils cherchent à établir les faits ou, au contraire, à montrer que les informations manquent de fondement et s'efforcent d'identifier les sources et les réseaux qui ont l'habitude de produire et ou de diffuser de fausses informations. Ils n'en sont pas moins pris dans des tensions complexes. D'abord, certains groupes sont financés par les plateformes elles-mêmes ce qui fragilise leur indépendance. La vérification des faits est en effet coûteuse dès lors qu'elle implique d'entretenir d'importantes bases de données et de rémunérer des équipes qualifiées pour les gérer. D'autre part, ces vérificateurs n'ont pas accès à la totalité des informations qui circulent sur les plateformes – ils ne peuvent voir, en particulier, les informations partagées au sein de groupe privés ou de messageries – ce qui constitue un grand nombre d'angles morts. L'Union Européenne promeut en ce sens des échanges plus fluides d'informations entre les plateformes et les vérificateurs. L'autorité sous l'égide de laquelle les vérificateurs agissent peut en outre être discutée et générer chez l'utilisateur le rejet de la qualification du contenu en « désinformation » ou « mésinformation ». Ainsi, l'utilisateur pourrait considérer que la volonté même de cacher l'information, émanant d'une autorité contestée, atteste de sa légitimité. Enfin, de nombreuses associations de vérificateurs sont constituées principalement de journalistes, qui peuvent être désarmés face à certaines informations ou controverses d'ordre scientifiques, en particulier pendant la crise Covid-19.

[51] Communication de la Commission européenne Lutter contre la désinformation concernant la COVID-19 préc., partie 5.2. Soutien aux vérificateurs de faits et aux chercheurs, p.11.

Recommandations :

2.3 Faciliter le transfert d'informations entre les plateformes et les vérificateurs.

2.4 Renforcer le pluralisme des équipes de vérificateurs afin que les chercheurs et la société civile puisse y être représentés.

S'agissant tout particulièrement de la promotion de certains contenus, il est également possible d'interroger la neutralité de l'État dès lors que les informations qu'il promeut sont aussi celles qui légitiment l'action du gouvernement. Laisser les entreprises en discussions exclusives avec lui fait courir d'importants risques de censure. Les arguments qui questionneraient certaines des décisions politiques du gouvernement pourraient être écartés ou supprimés injustement. L'exemple de la page « Désinfox information » en est une alerte. Celle-ci a été mise en place par le gouvernement, mais retirée quelques heures après le dépôt d'un référé liberté auprès du Conseil d'État par le syndicat national des journalistes qui y voyait une « atteinte grave au pluralisme"[52].

Par ailleurs, cette exclusivité risquerait d'engendrer un certain nombre d'ambiguïtés dans les relations entre ces plateformes et les autorités étatiques, en particulier celles avec le gouvernement. Les plateformes pourraient par exemple avoir recours au gouvernement pour valider ou modérer certaines informations, et ce dernier leur demander de promouvoir certains contenus visant à lutter contre la crise sanitaire. Il existerait alors un réel risque de connivence qui fournirait aux plateformes des appuis qu'elles pourraient mobiliser lorsqu'il serait question de contrôler leurs pratiques dans d'autres domaines (s'agissant par exemple de leurs pratiques concernant l'information des utilisateurs sur leurs modes de fonctionnement).

Recommandation :

2.5 Publier les mécanismes de modération de contenus mis en œuvre lors de la crise sanitaire par les plateformes, en particulier ceux qui garantissent la transparence des interactions entre ces opérateurs et les autorités publiques, et exercer un contrôle *ex post* de ces mécanismes par l'autorité compétente, dont le juge en tant que garant des libertés individuelles.

Par ailleurs, la crise sanitaire que nous traversons a la particularité d'être, à un niveau rarement atteint, perçue à travers quantité de chiffres et des statistiques pour une très grande part produits par le service statistique public (SSP), comme le nombre de morts, de personnes infectées, de personnes soignées, à l'hôpital, dans les EHPAD, en population générale. La plupart des mesures politiques, des discours et des réflexions individuelles sur cette épidémie est orientée et confortée par des outils quantitatifs qui reposent sur des définitions et des méthodes qui en spécifient la portée à l'image du nombre de morts communiqué, qui n'est, au mieux, qu'une approximation de la réalité. Les limites de la

52 refere-liberte---04-05-2020.pdf, demande rejetée par l'ord. Conseil d'État, 8 juin 2020 relevant que "le Premier ministre a supprimé cette page Internet, à compter du 5 mai 2020, soit postérieurement à l'introduction de la requête » ce dont il résulte que « les conclusions de cette requête ont perdu leur objet et il n'y a plus lieu d'y statuer » tout en condamnant l'État aux frais de procédure – v. également l'intervention du Ministre de la Culture Franck Riester annonçant le retrait de cette page : Questions au Gouvernement, 5 mai 2020.

portée des outils statistiques ne sont que rarement mises en avant alors que ces chiffres sont relayés très largement. Le manque de mise en contexte de ces chiffres peut être source d'interprétations participant à une forme de désinformation.

Recommandations :

2.6 Accompagner la communication des statistiques relatives à l'épidémie d'un discours méthodologique rappelant notamment le contexte et les limites des résultats obtenus.

2.7 Publier des réflexions non seulement sur les méthodes de production des statistiques, mais aussi sur leurs usages et les transformations qu'elles subissent au fur et à mesure de ces réappropriations : comment elles sont utilisées, transmises et parfois déformées, comment elles influencent les comportements du gouvernement ou du public.

Enfin, le recours à des autorités établies pour promouvoir des contenus scientifiques présentés comme certains ne doit pas conduire à sous-évaluer le caractère controversé de ceux-ci[53]. L'OMS, par exemple, semble admise comme une source sûre de résultats scientifiques par les plateformes, alors que d'autres autorités scientifiques la contestent, parfois à bon droit[54]. D'autres acteurs, comme les utilisateurs, les scientifiques ou encore les associations pourraient dès lors être impliqués dans la sélection des informations mises en avant[55].

[53] Sur les enjeux éthiques liés aux contre-vérités scientifiques, la post-vérité et la communication de la science dans la sphère publique, v. déjà l'avis n°2018-37 du COMETS « Quelles nouvelles responsabilités pour les chercheurs à l'heure des débats sur la post-vérité ? » publié le 12 avril 2018.

[54] A cet égard, v. la tribune publiée dans Le Monde et signée par de nombreuses autorités qui appelle à développer le « le Forum sur l'information et la démocratie, créé en novembre 2019 par onze organisations, think tanks et centres de recherche de neuf pays, pour mettre en œuvre le Partenariat » entre les plateformes et les acteurs sociaux (« Nous appelons les géants du Web à un sursaut décisif pour le droit à l'information fiable », Le Monde, 02/05/2020. Signée entre autres par Joseph Stiglitz, Christophe Deloire et Shirin Ebadi).

[55] En ce sens, v. Créer un cadre français de responsabilisation des réseaux sociaux : agir en France avec une ambition européenne, rapport préc.

ANNEXES

Personnes auditionnées

- **Serge Abiteboul,** membre de la mission de régulation des réseaux (2019) et membre du collège de l'ARCEP
- **Lucien Castex**, Secrétaire général d'Internet Society France
- **Guillaume Champeau,** directeur du service Éthique et Affaires juridiques, **Leonard Cox,** vice-président des Affaires publiques et RSE, **Jean-Claude Ghinozzi,** Président-directeur général **et Sébastien Ménard**, Conseiller en stratégie, QWANT
- **Guillaume Goubert,** directeur du journal La Croix
- **Béatrice Oeuvrard,** chargée des affaires publiques, Facebook
- **Audrey Herblin-Stoop,** chargée des affaires publiques, Twitter
- **Jonathan Parienté**, journaliste au Monde, chef du service des Décodeurs
- **Ramón Ruti**, co-fondateur et CTO de Storyzy

Composition du groupe de travail ayant contribué à l'élaboration de ce document

Laurence Devillers	Claude Kirchner
Emmanuel Didier*	Jérôme Perrin
Karine Dognin-Sauze	Catherine Tessier
Christine Froidevaux	Serena Villata*
Eric Germain	Célia Zolynski*
Alexei Grinbaum	
Jeany Jean-Baptiste	**corapporteurs*

Version révisée le 1er octobre 2020

La publication de ce bulletin a été validée le 8 juillet 2020 lors de l'assemblée plénière incluant Emmanuel Didier (membre du CCNE) en tant qu'invité avec 16 voix pour, 1 voix contre et 2 abstentions.

Bulletin de veille n°3 :

ENJEUX D'ÉTHIQUE LIÉS AUX OUTILS NUMÉRIQUES EN TÉLÉMÉDECINE ET TÉLÉSOIN DANS LE CONTEXTE DE LA COVID-19

Bulletin de veille
Publié le 21 juillet 2020

https://www.ccne-ethique.fr/fr/actualites/comite-national-pilote-dethique-du-numerique-bulletin-de-veille-ndeg3

COMMUNIQUÉ DE PRESSE

Le recours à la télémédecine et au télésoin s'est accru de façon spectaculaire durant la période de confinement lié à l'épidémie de SARS-CoV-2. Si ce contexte a entraîné une forte augmentation de la demande en télémédecine et en particulier du recours à la téléconsultation, cet accroissement a surtout été possible car le système de santé y était préparé, des outils numériques d'échange et de partage d'informations étaient disponibles, et les pouvoirs publics ont pris des mesures dérogatoires de l'exercice de la télémédecine pour faciliter la continuité des soins.

Dans ce bulletin de veille[56], le Comité national pilote d'éthique du numérique (CNPEN) s'interroge sur l'évolution de cette pratique dans la suite de cette pandémie et au-delà. Il met en exergue l'intérêt et la complexité de ces nouvelles pratiques médicales et discute les enjeux que fait naître la combinaison des exigences médicales et numériques.

Le bulletin explicite des tensions éthiques relatives à la télémédecine et au télésoin qui ont été accentuées durant la crise, notamment celles qui sont relatives au secret médical et au respect de la confidentialité, au consentement et à l'information du patient ou encore à la fragilisation possible de notre système de soins par une éventuelle mise en cause des principes de solidarité et de mutualisation sur lesquels il repose.

Dix-sept points de vigilance sont tirés de cette analyse qu'il conviendra de poursuivre notamment à travers une délibération la plus ouverte possible sur les conséquences humaines des pratiques médicales utilisant les objets numériques.

[56] Le premier bulletin (https://www.ccne-ethique.fr/fr/actualites/comite-national-pilote-dethique-du-numerique-bulletin-de-veille-ndeg1) portait d'une part sur l'usage d'outils numérique dans le cadre d'actions de fraternité et sur les outils de traçage numérique d'autre part. Un second bulletin portant sur les enjeux d'éthique dans la lutte contre la désinformation et la mésinformation paraît le 21 juillet 2020.

ENJEUX D'ÉTHIQUE LIÉS AUX OUTILS NUMÉRIQUES EN TÉLÉMÉDECINE ET TÉLÉSOIN DANS LE CONTEXTE DE LA COVID-19

Nous avons assisté dès le début de la période de confinement à un accroissement particulièrement important des actes relevant de la télémédecine ou du télésoin : en trois semaines, leur nombre a été multiplié par un facteur 100, passant de 10 000 par semaine à près d'un million. Ce développement du recours à la téléconsultation a été rendu possible car lorsque la demande a brutalement augmenté du fait notamment du confinement, le système de santé y était préparé, des outils numériques d'échange et de partage d'informations de bonne qualité étaient disponibles (réseaux, matériels, logiciels, plates-formes, etc.), et les pouvoirs publics ont pris des mesures dérogatoires de l'exercice de la télémédecine pour faciliter la continuité des soins.

L'ensemble de ces points sont précisément documentés dans ce troisième bulletin de veille du Comité national pilote d'éthique du numérique (CNPEN). Le sujet de la télémédecine relevant à la fois des domaines du numérique et de la santé, ce bulletin a été élaboré par un groupe de travail associant des membres du CCNE pour les sciences de la vie et de la santé et des membres du CNPEN. Il met en exergue l'intérêt et la complexité de ces nouvelles pratiques médicales, discute les enjeux que fait naître la combinaison des exigences médicales et numériques et énonce dix-sept points de vigilance permettant de les prendre en compte. Citons notamment l'importance de la sensibilisation des soignants aux enjeux d'éthiques de l'usage des outils numériques, la prise en compte des inégalités d'accès à la télémédecine ou encore l'importance de veiller à n'utiliser, dans un contexte de soin, que des outils de communication de données sécurisés et respectant la réglementation relative à l'hébergement et au traitement des données de santé.

L'utilisation massive de la télémédecine pendant cette épidémie nous amène à nous interroger sur l'évolution de cette pratique dans les différentes phases de déconfinement, non seulement en prévision de crises ultérieures, mais aussi dans la pratique courante une fois l'épidémie résolue.

Raja Chatila, Laure Coulombel, Christine Froidevaux

Rapporteurs du groupe de travail

Claude Kirchner

Directeur du comité national pilote d'éthique du numérique

I. Déploiement d'outils numériques en télémédecine et télésoin pendant la crise de la COVID-19

La période de confinement lors de l'épidémie de SARS-CoV-2 a bouleversé les pratiques de soins et, notamment, l'accès à une consultation médicale pour les patients, qu'ils soient atteints de formes non graves de la COVID-19, ou d'autres maladies nécessitant une prise en charge ou un suivi médical. Ainsi ont été observées, d'une part, la chute de l'activité des cabinets médicaux[57] dès l'annonce du confinement, accentuée par la réorganisation des services hospitaliers en faveur des patients COVID-19 et, d'autre part, l'augmentation significative de la téléconsultation (au sens large), ce recours n'ayant que partiellement comblé la diminution très importante des recours aux soins.

A. La télémédecine et le télésoin avant la crise de la COVID-19

La ***télémédecine***, au sens de l'article L6316-1 du Code de la santé publique est « *une forme de pratique médicale à distance utilisant les technologies de l'information et de la communication* ». Elle inclut cinq actes selon le décret de 2010[58] : la téléconsultation, la téléexpertise (quand un médecin sollicite à distance l'avis d'un autre médecin), la télésurveillance (permet à un professionnel médical d'interpréter à distance les données nécessaires à la prise en charge médicale d'un patient et, le cas échéant, de prendre les décisions appropriées), la téléassistance (permet à un professionnel médical d'assister à distance un autre professionnel de santé au cours de la réalisation d'un acte), et la régulation médicale (le « 15 »). Son déploiement s'accélère depuis fin 2018, date à laquelle les actes de téléconsultation et de téléexpertise sont entrés dans le droit commun au remboursement par l'Assurance Maladie, et sont intégrés au parcours de soin coordonné (c'est-à-dire avec une orientation initiée par le médecin traitant)[59].

Les ***télésoins*** sont une pratique de soins à distance, distincte de la télémédecine. Ils sont intégrées dans la loi de santé votée en juillet 2019, mais dont les décrets d'application ne sont pas tous parus à ce jour (17 juillet 2020). Ils utilisent les technologies de l'information et de la communication, et mettent en rapport un patient avec un ou plusieurs pharmaciens ou auxiliaires médicaux[60] dans l'exercice de leurs compétences[61].

[57] Baisse de 40% pour les cabinets médicaux de soins primaires (de 30% après compensation par les téléconsultations). Baisse de 70% pour les cabinets de spécialistes (données de la CNAM) (voir rapport au ministre chargé de la Sécurité sociale et au Parlement sur l'évolution des charges et produits de l'Assurance maladie au titre de 2021- juillet 2020) https://assurance-maladie.ameli.fr/sites/default/files/rapport-charges-et-produits-2021.pdf

[58] Décret n° 2010-1229 du 19 octobre 2010 relatif à la télémédecine

[59] https://www.ameli.fr/fileadmin/user_upload/documents/Dossier-de-presse_Teleconsultation_12092018.pdf

[60] Infirmier(e)s, orthophonistes, ergothérapeutes, psychomotriciens, masseurs-kinésithérapeutes. https://solidarites-sante.gouv.fr/IMG/pdf/covid-19-telesuivi-infirmier.pdf

[61] Le cadre juridique des actes de télésoins sera défini dans la nouvelle loi relative à l'organisation et à la transformation du système de santé : https://www.senat.fr/rap/l18-524/l18-52419.html

Le développement de la télémédecine était inférieur aux attentes de l'Assurance Maladie62,63, en dépit des expérimentations menées depuis plusieurs années[64], et inégal sur le territoire (44% des téléconsultations en Île-de-France).

Plus récemment, une ***stratégie de transformation du système de santé a été mise en œuvre*** et a affiché une ambition numérique, notamment à travers la loi de transformation du système de santé du 24 juillet 2019[65]. Le plan « Ma Santé 2022 » prévoit ainsi le déploiement d'outils numériques dans le parcours de soin dont la télémédecine et les télésoins, l'institution d'un espace numérique de santé pour chaque citoyen intégrant son dossier médical partagé (DMP) et permettant des échanges sécurisés avec les professionnels et les établissements, ainsi que la création d'une plate-forme des données de santé (*Health Data Hub*).

La ***téléconsultation*** est une pratique médicale qui relève des mêmes règles déontologiques qu'une prise en charge au cabinet du médecin, et elle doit avoir le même rendu, même si les modalités de questionnement et d'écoute du patient diffèrent. Comme dans son cabinet, le médecin est responsable de tout acte ou prescription découlant d'une téléconsultation ; il doit notamment, s'il le juge nécessaire à l'établissement de son diagnostic, mettre fin à la téléconsultation et organiser une visite au cabinet d'un médecin local. Cette pratique peut, ou non, être accompagnée par un soignant, par exemple quand elle a lieu dans un EHPAD. Elle peut, ou non, utiliser un dispositif connecté, tel un stéthoscope ou un oxymètre. Une cabine fixe de téléconsultation disposant des logiciels et équipements connectés et installée dans divers locaux, des entreprises ou des pharmacies peut aussi être utilisée.

Comme indiqué sur le site du ministère de la Santé et des Solidarités[66], la téléconsultation est très codifiée dans le cadre du parcours de soins coordonnés, et « la pertinence d'une prise en charge à distance plutôt qu'en présentiel est appréciée par le médecin », c'est-à-dire qu'il lui revient de la proposer au patient, et de discerner dans quels cas elle est appropriée et dans quels cas elle ne l'est pas. La Haute autorité de santé rappelle que le recours à la téléconsultation « relève d'une décision partagée du patient et du professionnel médical qui va réaliser la téléconsultation »[67] et énumère un certain nombre de critères d'éligibilité.

---

[62] *La gouvernance de la télémédecine face à l'organisation libérale des soins.* Florence Gallois, Amandine Rauly. L'Harmattan | « Marché et organisations » 2020/2 n° 38 | pages 37 à 60

[63] Cour des Comptes, rapport public annuel 2018, tome 2 : Les services publics numériques en santé. Cour des comptes, Rapport sur l'application des lois de financement de la sécurité sociale pour 2017, chapitre VII, La télémédecine : une stratégie cohérente à mettre en œuvre, p.295-330.

[64] Le nombre moyen d'actes se situait en-dessous de 200 actes par semaine en 2018, 700 à la mi-février 2019, 3 300 en septembre, pour un total de 60 000 téléconsultations fin août 2019. Les pouvoirs publics avaient anticipé 500 000 téléconsultations en 2019 et 1,3 million en 2021. Voir documents cités en [1] et [6].

[65] https://solidarites-sante.gouv.fr/IMG/pdf/190425_dossier_presse_masante2022_ok.pdf, et https://www.legifrance.gouv.fr/affichLoiPreparation.do?idDocument=JORFDOLE000038124322&type=general&typeLoi=proj&legislature=15

[66] https://solidarites-sante.gouv.fr/soins-et-maladies/prises-en-charge-specialisees/telemedecine/la-teleconsultation/article/generalites

[67] https://www.has-sante.fr/jcms/c_2844641/fr/qualite-et-securite-des-actes-de-teleconsultation-et-de-teleexpertise

Recours massif à la télémédecine pendant la crise

Le nombre de consultations réalisées à distance (que nous assimilons dans ce texte à des téléconsultations) et remboursées par la CNAM a considérablement augmenté depuis le début du confinement68, même si l'analyse des outils numériques utilisés et des justifications médicales ne permet pas à ce jour de distinguer celles qui ont réellement utilisé un moyen de vidéotransmission (téléconsultations référencées) des consultations par téléphone (qui ont été assimilées à une téléconsultation). Parallèlement à ces chiffres institutionnels, la plate-forme Doctolib annonce également une augmentation d'un facteur 100 des rendez-vous de téléconsultation au 22 avril 202069. Cette augmentation a également été constatée par les plates-formes développées par les organismes complémentaires de l'Assurance Maladie (MesDocteurs.com)70.

Plusieurs éléments ont facilité le recours à la téléconsultation pendant la crise :

- *Le contexte épidémique de la COVID-19*. Le médecin comme le patient doivent se protéger d'un risque de contamination, particulièrement s'il existe une pénurie de masques. L'écran et la distance - jusque-là plutôt considérés comme des obstacles au « contact humain », essentiel à la relation médecin-patient - protègent d'une contamination du médecin par le patient, du patient par le médecin[71] ou d'un patient par un autre patient, du fait de l'absence d'examen clinique ou de contacts avec d'autres personnes dans une salle d'attente ou encore lors des déplacements. Une communication à distance avec le médecin pourrait apparaître dans ce contexte de la pandémie comme la garantie d'une continuité de l'accès aux soins, mise en péril par la crainte d'une contamination lors d'une consultation en présentiel ou le manque de disponibilité du médecin traitant.
- Les mesures dérogatoires[72] instituées par les autorités sanitaires. Elles ont joué un rôle fondamental pour faciliter l'accès aux consultations à distance (téléconsultation et téléphone) et inciter les patients à y recourir. Toutefois ces mesures n'ont que partiellement atténué l'évitement du recours aux soins[73] en ne

---

68 « 80 000 téléconsultations ont été facturées à l'Assurance Maladie la semaine du 16 mars 2020, puis 486 369 du 23 au 29 mars 2020 et plus de 1 million début avril. L'Assurance Maladie en comptabilisait moins de 10 000 par semaine jusque début mars. Les téléconsultations constituaient en avril 2020 plus de 11 % de l'ensemble des consultations contre moins de 1 % avant la crise ».
Voir : https://www.ameli.fr/fileadmin/user_upload/documents/20200331_-CP_Teleconsultations_Covid_19.pdf

69 Dossier de presse du 22 avril : 2,5 millions de RV de téléconsultations en un mois et une augmentation de 1 000 consultations par jour à plus de 100 000, 800 000 patients ayant effectué au moins une téléconsultation *via* le site.

70 « L'entreprise de télémédecine MesDocteurs a vu les inscriptions de professionnels de santé à son service de téléconsultation « AvecMonDoc.com » progresser de 400% pendant la période de confinement (entre le 16 mars et le 11 mai). Le volume de téléconsultations non programmées a lui connu une progression de « +700% » pendant la même période. Depuis la levée progressive des mesures de confinement, le volume de téléconsultations non programmées a baissé de 50% ». (site TicSanté, 18 juin 2020)

71 La transmission involontaire d'infections par les soignants est connue depuis le milieu du XIXème siècle grâce à Ignace Philippe Semmelweis. Cet obstétricien hongrois a permis de réduire drastiquement le taux de mortalité dans les maternités en imposant un simple geste : le lavage des mains.

72 Les mesures dérogatoires : le remboursement à 100% des communications à distance, y compris par téléphone si les patients n'ont pas accès à des outils numériques ou internet, et y compris *via* des outils de communication grand public non référencés ; le recours à une téléconsultation à l'initiative du patient et même si elle ne s'inscrit par dans le parcours de soins coordonnés, donc sans que le patient soit connu du médecin consultant.

73 https://lesgeneralistes-csmf.fr/2020/04/27/attention-a-la-bombe-a-retardement-post-epidemie-les-medecins-face-aux-dommages-collateraux-du-covid-19

compensant pas la diminution, dès le début du confinement, des consultations pour d'autres maladies que la COVID-19, en particulier de spécialistes.

- La diversité et la pratique des outils numériques de communication et de partage d'informations.

Parallèlement à la téléconsultation médicale, les autorités sanitaires ont également permis de manière dérogatoire l'exercice des télésoins, permettant en particulier un suivi régulier des maladies chroniques.

Une autre forme de soins à distance pendant la crise est le télésuivi des patients COVID-19 à domicile sous forme de questionnaires numériques (Covidom à Paris, MHLINK à Montpellier ou COVIDAPHM à Marseille). D'autres applications existent utilisant un questionnaire d'autoévaluation et un algorithme d'orientation des patients possiblement infectés (site maladieCoronavirus.fr).

Enjeux d'éthique des outils numériques en télémédecine et télésoin

Le basculement rapide vers une consultation à distance auquel les patients, comme les médecins, ont été contraints pour répondre à l'urgence sanitaire justifie de s'interroger sur le rapport bénéfices-risques de cet exercice de la médecine différent des consultations traditionnelles au cabinet du médecin, notamment lorsque des solutions numériques sont utilisées. Ce débat est d'autant plus nécessaire que l'attitude des citoyens se modifie et qu'avec la banalisation de l'usage du numérique se renforce la tendance au consumérisme médical, suscitant, en dehors de la consultation programmée, une demande de conseil médical rapide via les outils de communication numériques. Cette réflexion – qui dépasse le cadre de ce bulletin – est importante en ce temps de déconfinement alors qu'une discussion sur l'avenir des mesures dérogatoires à l'origine de cette envolée des téléconsultations est en cours[74,75], et qu'une meilleure intégration des outils numériques dans la pratique médicale est inscrite dans la future loi de santé.

Un premier enjeu d'éthique est relatif à l'utilisation par les soignants de solutions numériques susceptibles d'entraîner des risques pour les patients. Celles-ci mettent en jeu des critères souvent méconnus, particulièrement en temps de crise. Le ministère de la Santé et des Solidarités a ainsi référencé - dans l'urgence - une centaine d'outils de télésanté disponibles, essentiellement des outils de vidéotransmission (liste établie le 18 mars, et mise à jour le 4 mai), et proposé une liste de critères pour les sélectionner, tels que la facilité d'installation et la sécurisation[76]. Au-delà des choix reposant sur les fonctionnalités techniques souhaitées, le recours à de tels outils numériques soulève des enjeux d'ordre éthique que nous examinons dans la suite. Les risques d'atteinte à la vie privée ou relatifs à la protection des données ont par exemple été exacerbés pendant la crise en raison des mesures dérogatoires.

---

[74] Voir le rapport cité en [1]

[75] Société Française de santé digitale, « Télésanté « post Covid-19 » en France. Dix préconisations pour accélérer la télésanté » Juillet 2020 - https://sfsd-umd.fr/wp-content/uploads/2020/07/Position-Paper-SFSD-10-préconisations-pour-la-télésante-juillet-2020.pdf

[76] https://solidarites-sante.gouv.fr/soins-et-maladies/maladies/maladies-infectieuses/coronavirus/professionnels-de-sante/article/teleconsultation-et-covid-19-qui-peut-pratiquer-a-distance-et-comment

Au-delà des aspects organisationnels et techniques de la téléconsultation, les consultations à distance en temps de crise sanitaire ont nourri une réflexion éthique déjà en cours, issue du bouleversement des pratiques de soin auxquelles sont confrontés les soignants, comme les patients, avec l'avènement des outils numériques. Cette évolution parfois redoutée comme le serait une « industrialisation » du soin, peut fragiliser les principes de l'éthique médicale. Il est essentiel d'en tenir compte. Il serait intéressant, dans le contexte d'après-crise, de discuter des cas d'usage pertinents de la télémédecine et du télésoin dans la prise en charge médicale, et des aménagements des modalités de recours aux solutions numériques afin qu'elles garantissent la sécurité des échanges de données tout en ne les entravant pas.

Un autre enjeu d'éthique majeur est l'exigence d'une information de qualité à la disposition du patient relative aux conditions du recours à la télémédecine, à ses bénéfices comme à ses risques, afin de lui permettre d'élaborer le cas échéant son consentement libre et éclairé à ces nouvelles pratiques, sans risque de discrimination ou de pénalisation. Enfin, avec la crise on a assisté au développement de l'offre de plates-formes privées de téléconsultation se situant hors du parcours de soin coordonné, pouvant mettre en danger le principe de solidarité et de mutualisation des risques, fragiliser les relations suivies médecin-patient, et avoir des conséquences négatives pour le patient si elles sont de qualité insuffisante.

II. Points de vigilance concernant le déploiement de la télémédecine et du télésoin en temps de crise et en sortie de crise

A. La formation des soignants et l'information des patients relatives à la téléconsultation

La téléconsultation, inscrite réglementairement dans le cadre du parcours de soins coordonnés, est, comme la téléexpertise, une pratique médicale très codifiée[77] pour laquelle il faut être formé, connaître les aspects réglementaires, certaines spécificités déontologiques, et les aspects techniques (notamment les relations avec le gestionnaire de la plate-forme qui fournit les solutions numériques sécurisées).

Si l'offre est importante (90 solutions numériques de téléconsultation recensées par le ministère au 12 juin 2020 à partir d'une auto-déclaration par les éditeurs de solutions[78]), les critères de choix peuvent ne pas être connus, et la communication institutionnelle ne pas être très performante auprès des acteurs de terrain. Compte tenu du faible pourcentage de médecins ayant expérimenté la téléconsultation avant la crise, on peut émettre l'hypothèse selon laquelle un certain nombre de soignants peu familiarisés avec cette pratique médicale ont pu hésiter à l'utiliser[79].

« Les limites de la démocratisation de la télémédecine tenaient à un manque de formation et d'accompagnement des professionnels de santé »[80]. Il importe donc de proposer aux soignants des formations leur permettant d'acquérir les connaissances nécessaires pour maîtriser les pratiques de télémédecine sur le plan informatique et réglementaire (sécurisation des canaux de communication, confidentialité des données, contrat de sous-traitance avec le gestionnaire de plate-forme, etc.) et ce, en situation normale ou de crise.

Au-delà de la télémédecine, on ne peut qu'insister sur l'importance de l'exigence de formation au numérique et par le numérique pendant le cursus universitaire des professionnels de santé.

Selon l'enquête Odoxa publiée en janvier 2020, 29% des patients qui ont expérimenté une téléconsultation sont insatisfaits, les aspects techniques constituant le principal vecteur de leur satisfaction ou insatisfaction[81]. La diffusion large d'une information efficace et simple relative à la démarche d'utilisation de la téléconsultation auprès des patients s'avère donc également nécessaire.

---

[77] Voir le guide des bonnes pratiques édité par la Haute autorité de santé (HAS) (mai 2019). Le remboursement est régi par des règles strictes établies par l'avenant 6 de la convention signée par la CNAM (2016). Il faut au préalable avoir déjà eu un rendez-vous physique avec le médecin au cours des douze derniers mois, que la téléconsultation respecte le « parcours de soin » comme une consultation classique et que les moyens techniques utilisés soient sécurisés. La consultation à distance doit toujours s'effectuer dans le cadre d'une « *organisation territoriale* ».

[78] https://solidarites-sante.gouv.fr/soins-et-maladies/maladies/maladies-infectieuses/coronavirus/professionnels-de-sante/article/teleconsultation-et-covid-19-qui-peut-pratiquer-a-distance-et-comment

[79] Selon l'enquête Odoxa publiée le 27 janvier 2020, http://www.odoxa.fr/sondage/panorama-telemedecine-aujourdhui-perspectives-lavenir, les soucis techniques (son, image, connexion) pointés dans les réponses au questionnaire expliquent sans doute que la téléconsultation ne soit pas davantage inscrite dans les pratiques futures des professionnels de santé.

[80] Nathalie Salles, nov. 2019 : https://sfgg.org/espace-presse/interviews/que-peut-la-telemedecine-pour-les-patients-ages-par-nathalie-salles-presidente-du-conseil-scientifique-de-la-sfgg-et-presidente-de-la-societe-francaise-de-sante-digitale/

[81] Selon l'enquête Odoxa citée en [21], 80% des Français savent ce qu'est une téléconsultation, mais seuls 6% en ont expérimenté une.

Points de vigilance :

1. Proposer des formations aux pratiques professionnelles de télémédecine à destination des soignants, portant sur les aspects techniques et sur les spécificités de cette nouvelle pratique médicale.
2. Sensibiliser les soignants aux enjeux éthiques de l'usage des outils numériques.
3. Fournir une information explicite aux patients sur les modalités de la téléconsultation et les enjeux éthiques de ces outils numériques, et les accompagner dans l'accès et l'usage de ces outils.

Le respect de l'autonomie des patients et le recueil du consentement libre et éclairé

Comme pour toute offre de soin, il est important que le patient soit informé des conditions de la téléconsultation et puisse y consentir librement et de façon éclairée lorsqu'elle lui est proposée. Dans le cas de la télémédecine, le consentement du patient au soin inclut son acceptation de l'acte médical et son acceptation que cet acte soit réalisé à distance. Le patient accepte ainsi que ses données numériques soient partagées et traitées par différents intervenants. Il doit donc être informé des conditions de traitement et de protection de ses données personnelles et de leur devenir. La déontologie du médecin et sa responsabilité lui imposent de s'assurer de la sécurisation de la transmission des données et de la préservation de leur confidentialité. Le consentement du patient est indispensable à la relation de confiance avec le médecin qui favorise son adhésion à la fois au diagnostic posé et au traitement proposé. Cette relation de confiance, habituelle avec le médecin traitant utilisant une téléconsultation, peut s'avérer plus délicate en cas de primo-consultation ou si la téléconsultation fait intervenir un médecin qui ne connait pas le patient (ce qu'ont rendu possible les mesures dérogatoires). Le choix des personnes qui ne souhaitent pas bénéficier d'une téléconsultation doit être respecté sans que cela affecte la qualité de leur prise en charge médicale, qui doit pouvoir alors se faire dans le cadre d'une consultation classique.

Dans le cas où le patient n'aurait pas d'autre possibilité d'accès à un médecin que *via* une téléconsultation, un manque de confiance, induit par exemple par l'absence de relation humaine physique, pourrait l'amener à douter de la pertinence du diagnostic. Le refus de la prescription qui pourrait s'en suivre serait préjudiciable au patient voire, dans le cas d'une maladie contagieuse, à la collectivité.

Points de vigilance :

4. Veiller à ce que, en dépit des contraintes liées à la situation d'urgence sanitaire et à l'utilisation de dispositifs de communication à distance, l'information et le recueil d'un consentement libre et éclairé du patient soient respectés. Une attention particulière concerne les données collectées et conservées, même temporairement, sur une plate-forme.
5. Sensibiliser l'ensemble des intervenants à l'importance de bien identifier les conditions et les finalités du traitement des données recueillies pendant une téléconsultation ou

des télésoins (objectifs de recherche, par exemple) et de s'assurer de la qualité et du statut des prestataires associés (publics, privés, nationaux ou étrangers).

6. Veiller à ce que les patients opposés à la téléconsultation ne subissent ni discrimination, ni pénalisation sur le plan de la qualité de leur prise en charge médicale.

L'équité dans l'accès aux actes de télémédecine

Si la télémédecine favorise un accès plus facile aux soins, son recours peut toutefois s'avérer limité, voire discriminatoire pour certaines personnes :

- qui ne sont pas équipées - ne peuvent ou ne souhaitent pas - d'équipement informatique, ou qui disposent d'un équipement obsolète ;

- qui ne bénéficient pas des connaissances nécessaires pour utiliser leur système informatique, ou pour s'approprier l'information concernant l'organisation d'une téléconsultation ;

- qui vivent dans un logement trop exigu pour pouvoir s'isoler et parler au médecin dans des conditions d'intimité comparables à celles d'un cabinet médical. Ce problème est aggravé en période de confinement et dans les phases de déconfinement progressif, y compris en raison du télétravail avec la surutilisation des espaces domestiques ;

- qui ne consultent que rarement un médecin. Dans le contexte de la pandémie, rappelons que les personnes les plus exposées (atteintes de maladies mentales, en grande précarité, désocialisées ou migrantes etc.), éprouvent plus que d'autres une difficulté à établir un lien avec les intervenants médicaux et ne bénéficient souvent d'aucun suivi médical.

Les conséquences de l'exclusion « numérique[82] » sont apparues encore plus évidentes pendant l'épidémie de COVID-19, les populations vulnérables mentionnées ci-dessus évoluant dans un contexte social qui les expose particulièrement aux risques de contamination. Les inégalités d'accès aux dispositifs numériques rencontrent les inégalités sociales, renforçant les inégalités sanitaires et territoriales[83].

[82] Concernant l'accès aux outils numériques, rappelons que d'après l'Insee[82], en France, en 2019, 12 % des personnes de 15 ans ou plus ne disposent d'aucun accès à Internet depuis leur domicile et 53 % des 75 ans ou plus n'ont pas accès à Internet), comme 34 % des personnes sans diplôme ou titulaires d'un certificat d'études primaires (CEP) et 16 % des plus modestes. https://www.insee.fr/fr/statistiques/4241397#consulter

[83] Voir bulletin de veille n°1 qui présente les questionnements éthiques liés à l'usage des outils numériques dans le cadre d'actions de fraternité : https://www.ccne-ethique.fr/fr/actualites/comite-national-pilote-dethique-du-numerique-bulletin-de-veille-ndeg1

Point de vigilance :

7. Les inégalités d'accès à la télémédecine constituent un véritable enjeu d'éthique, en particulier s'agissant des populations en situation de précarité. Des actions concrètes pourraient permettre de réduire ce préjudice par exemple en développant des espaces dédiés à la téléconsultation, comme dans les pharmacies ou autres lieux de proximité, et/ou en faisant appel à des intermédiaires de proximité habitués à l'usage des outils informatiques comme certaines administrations locales, les auxiliaires de soin ou les associations.

La sécurisation, la confidentialité et l'interopérabilité des données

Les données de santé sont considérées comme « sensibles » et bénéficient à ce titre d'une protection spécifique, inscrite notamment dans la loi informatique et liberté (LIL 1978), le Code de la santé publique et le règlement général sur la protection des données (RGPD, transcrit dans la LIL modifiée). Sur cette question, l'éthique médicale et l'éthique de l'informatique se rejoignent autour des valeurs de confidentialité et de respect de la vie privée.

Dans le cadre de la téléconsultation, les exigences sont définies[84] : il importe de veiller à la confidentialité de l'échange avec le médecin, nécessaire au respect du secret médical et à l'établissement d'une relation de confiance entre le patient et le médecin. Cela suppose non seulement que le patient puisse s'isoler pour sa téléconsultation (ou être accompagné d'un professionnel tenu au respect du secret), mais aussi que le mode de communication utilisé pour cette téléconsultation soit sécurisé.

Le ministère des Solidarités et de la Santé rappelle que « les professionnels sont tenus d'utiliser des outils (qu'ils soient référencés ou non), respectant la réglementation relative à l'hébergement des données de santé (HDS) et la politique générale de sécurité des systèmes d'information en santé (PGS-SIS). Toutefois, en cas d'impossibilité et exclusivement dans le cadre de la réponse à l'épidémie de COVID-19, les professionnels peuvent utiliser d'autres outils (arrêté du 19 mars 2020) » [85].

Ainsi, à titre dérogatoire, pour faciliter la continuité des soins en période d'épidémie, les professionnels de santé ont pu, s'ils ne disposaient pas des équipements nécessaires à l'utilisation de dispositifs référencés et sécurisés, consulter *via* des outils numériques de communication « grand public »[86]. Cette ouverture a contribué à l'accroissement du nombre de téléconsultations. Il est important de rappeler que la sécurité et la confidentialité doivent être respectées en toute circonstance et que seuls les dispositifs agréés et sécurisés sont autorisés. Concernant la certification et l'accréditation des hébergeurs de santé, une consultation est actuellement en cours[87].

---

[84] « Disposer des outils de communication pour la téléconsultation ; Disposer des outils informatiques pour l'échange, le partage et le stockage des données : messagerie sécurisée de santé et/ou accès à une plate-forme d'échange sécurisée ; hébergeur de données de santé agréé ou certifié en cas d'externalisation des données ». (HAS, https://www.has-sante.fr/upload/docs/application/pdf/2019-07/fiche_memo_teleconsultation_et_teleexpertise_mise_en_oeuvre.pdf).

[85] https://solidarites-sante.gouv.fr/soins-et-maladies/maladies/maladies-infectieuses/coronavirus/professionnels-de-sante/article/teleconsultation-et-covid-19-qui-peut-pratiquer-a-distance-et-comment

[86] What's app, skype, Facetime, le téléphone et les messageries personnelles non sécurisées.

[87] https://participez.esante.gouv.fr/project/referentiel-hds-2020/presentation/introduction

La question se pose de façon plus générale d'adapter les moyens techniques aux situations d'urgence, où l'échange rapide de données ou de documents peut s'avérer primordial (par exemple lors d'actes de téléexpertise). Cette question se pose tout particulièrement pour la gestion de maladies graves nouvelles, par exemple les formes aiguës de COVID-19 : l'échange d'informations entre praticiens y est indispensable (téléassistance et téléexpertise) et la connaissance de l'histoire médicale d'un patient, nécessaire pour définir les critères de gravité et choisir un traitement ou des actions adaptées, est parfois difficile à reconstituer sans accès à son dossier médical[88]. L'interopérabilité des systèmes d'information est à ce titre essentielle.

La tension est alors inévitable entre le besoin de sécuriser la transmission de ces données - avec pour conséquence de complexifier la communication pour les patients comme pour les praticiens - et le risque d'abandon du recours aux moyens sécurisés en raison de difficultés techniques. Il est d'ailleurs habituel, dans une situation de crise, de mettre en balance la sécurité des communications avec le bénéfice pour la santé du patient ainsi que pour la santé publique, et donc de graduer les exigences de sécurité en fonction de l'urgence et du bénéfice pour le patient ou pour la collectivité.

La confidentialité des données est fondamentale, même si celles-ci ne sont pas directement identifiantes. Citons leur utilisation possible à des fins de recherche et d'innovation médicale. Dans le cas de la COVID-19, les connaissances cliniques et épidémiologiques sur cette maladie nouvelle reposent sur l'analyse des données des patients. Rappelons que malgré la situation d'urgence, l'utilisation des dossiers médicaux à des fins de recherche ne peut se faire que conformément au RGPD, en respectant les finalités et la durée de conservation des données annoncées, dans une balance entre intérêt général et respect de la vie privée du patient[89].

Les points de vigilance qui suivent sont très importants et rejoignent le cadre de la feuille de route « Accélérer le virage numérique » dont l'une des cinq orientations vise à « intensifier la sécurité et l'interopérabilité des systèmes d'information en santé »[90].

<u>Points de vigilance :</u>

8. En toutes circonstances, utiliser des outils de communication de données de santé sécurisés respectant la réglementation relative à leur hébergement et leur traitement.
9. Dès à présent informer sur les outils numériques sécurisés de communication existants pour la télémédecine et s'assurer de leur appropriation par les professionnels de santé et la population.
10. Veiller à concevoir des systèmes d'information interopérables ainsi que des outils de communication et des centres d'hébergement et de traitement d'informations souverains et sécurisés pour la télémédecine et les évaluer régulièrement de manière indépendante.

[88] Cela soulève la question du bien-fondé du Dossier Médical Partagé que nous n'abordons pas ici, car non spécifique à la crise pandémique.
[89] https://gdpr-info.eu/art-89-gdpr/
[90] https://solidarites-sante.gouv.fr/IMG/pdf/190425_dossier_presse_masante2022_ok.pdf.

11. Au-delà de l'urgence de la crise sanitaire, sensibiliser les citoyens aux risques associés au cheminement des données numériques et à l'exploitation des données collectées dans le cadre des téléconsultations à l'aide d'outils non sécurisés.

Les principes de solidarité et de mutualisation des risques

Les facilités de recours aux consultations à distance accordées par les mesures dérogatoires pendant l'épidémie de COVID-19 se sont accompagnées d'une offre accrue de solutions numériques par des entreprises privées ou le secteur assurantiel.

Une des mesures dérogatoires instituées pendant la crise COVID-19 permet un remboursement intégral de la téléconsultation. Cette mesure s'applique également aux actes hors parcours de soins coordonnés[91], donc sans remboursement intégral dans ce cas. Les plates-formes de consultations en ligne – qui se sont multipliées ces dernières années[92] – ont été très réactives du fait de ces facilités, certaines proposant notamment aux médecins d'utiliser gratuitement leurs services pendant la crise de la COVID-19. Cela peut être assimilable à une publicité à caractère commercial pour une offre de soins. Certains craignent aussi, à la faveur de cette crise, une accélération de ces pratiques qu'un rapport du Conseil national de l'Ordre des médecins[93] a qualifiée « d'ubérisation de la santé ». Il s'agit notamment du développement de plates-formes de téléconsultation financées par les organismes complémentaires d'assurance maladie (les Français qui ont souscrit un contrat de garantie pouvant bénéficier de quatre à six téléconsultations par an), ou de plates-formes commerciales indépendantes de ces organismes complémentaires et soumises à la concurrence. Il s'agit en général de prises en charge ponctuelles, à l'initiative du patient, concernant de petits risques, et qui ne sont pas prises en charge par l'Assurance Maladie dès lors qu'elles ne s'inscrivent pas dans une permanence des soins primaires territorialisée. Toutefois, leur rôle n'est pas complètement clarifié et la frontière entre les pratiques de téléconseil (qui sont exclues du cadre de la télémédecine) et celles de téléconsultation est encore floue.

Leur développement non maîtrisé pourrait représenter une offre parallèle de soins privés se développant à côté du parcours de soins coordonnés, pouvant porter atteinte au principe de la solidarité et de la mutualisation des risques sur lequel est fondé notre système de soins et d'assurance maladie. Cette offre parallèle pourrait introduire une rupture concurrentielle par exemple si une plate-forme effectuait des relances commerciales ou redirigeait un patient vers un soignant proposant la téléconsultation - ce qui pourrait être considéré comme un détournement de patientèle.

Une question fondamentale est celle de la qualité de cette prise en charge, dès lors qu'elle se situe hors du parcours de soins coordonnés.

---

[91] Le parcours de soin est coordonné par le médecin traitant ; la téléconsultation est hors parcours de soin si elle n'a pas été proposée au patient par son médecin traitant ou par un médecin avec lequel il l'a mis en relation, ou si elle est pratiquée hors du territoire de résidence.

[92] Qare, Consulib, Doctoconsult, Hellocare, Doctinet, MédecinDirect, CompuGroup Medical, etc.

[93] Rapport télémédecine et autres prestations médicales électroniques, fév. 2016 et « La télémédecine face au risque d'ubérisation des prestations médicales » : Rappel des positions du Conseil national de l'ordre des médecins, fév. 2018.

Point de vigilance :

12. Une exigence d'éthique est d'éviter le développement non maîtrisé du marché de la santé afin de respecter le principe de solidarité nationale sur lequel est fondé notre système de soins et d'assurance maladie. En particulier il convient de s'assurer que les plates-formes de téléconsultation respectent les obligations déontologiques et réglementaires qui s'appliquent à la prise en charge médicale.

Les questionnaires en ligne

Ce qu'a également révélé l'épidémie de COVID-19, c'est l'utilité du « télésuivi » à domicile. Face à l'épidémie, les hôpitaux ont proposé rapidement de tels outils[94] pour les patients « porteurs ou suspectés » d'infection par le coronavirus ne nécessitant pas d'hospitalisation ou après leur hospitalisation. L'Assistance publique-Hôpitaux de Paris (AP-HP) a lancé dès le 9 mars la solution gratuite Covidom[95]. Chaque jour, le patient confiné reçoit un questionnaire médical numérique auquel il répond. En fonction de ses réponses, l'application numérique génère des alertes, captées par un centre de télésurveillance médicale et renvoyées vers l'équipe soignante qui adapte le suivi et la prise en charge au besoin du patient. D'autres applications similaires ont été proposées dans d'autres régions[96]. La plate-forme de télésuivi Lifen Covid[97] permet de suivre à distance les malades en coopération avec leur médecin traitant, échangeant des informations de santé *via* une messagerie sécurisée. Pour toutes ces applications, la validation d'un médecin est nécessaire (médecin hospitalier, ou médecin traitant) afin que le patient puisse installer l'application. Toutefois, chaque version de ces différentes applications devrait être soumise à audit et validation pour permettre aux médecins et aux patients d'accepter avec confiance les propositions des programmes utilisés dans ces systèmes.

D'autres questionnaires en ligne visant à aider l'internaute à évaluer son état de santé relatif à la COVID-19 sont proposés sur le net, parfois sans garanties médicales. En répondant à ces questionnaires, les utilisateurs risquent d'être mal informés de leur état de santé, voire, en cas d'hameçonnage (*phishing*), de communiquer leurs informations personnelles de santé à des prestataires qui agiraient dans le seul but de commercialiser ces données.

Points de vigilance :

13. Soumettre à audit et validation les applications de questionnaires en ligne.

14. Lors d'un télésuivi par questionnaires numériques, garantir un contrôle interactif régulier entre le patient et un soignant.

---

[94] https://www.lequotidiendumedecin.fr/actus-medicales/esante/covid-19-des-chu-misent-sur-les-solutions-de-telesuivi

[95] https://www.service-public.fr/particuliers/actualites/A13927

[96] MyCHURennes à Rennes, CovidAPHM à Marseille, MHLINK à Montpellier (qui propose en outre des conseils)

[97] https://blog.lifen.fr/posts/fightcovid19-comment-preparer-le-deploiement-de-lifen-covid comme au CHU de Saint-Étienne et au CHR d'Orléans.

15. Veiller à sensibiliser les utilisateurs aux risques de diagnostic erroné ou d'usage abusif de leurs données personnelles lorsqu'ils répondent à des questionnaires en ligne sur la santé sans la médiation d'un médecin.

Les enjeux d'éthique liés aux objets connectés

Dans le cadre de l'épidémie de COVID-19, les objets connectés ont été peu utilisés alors qu'ils auraient pu, pour certains d'entre eux (tensiomètres, oxymètres, stéthoscopes, électrocardiographes etc.), apporter des informations complémentaires facilitant le diagnostic ou l'évaluation de la gravité de la maladie à distance et, pour d'autres, faciliter la prise en charge des maladies chroniques sans risque de contamination.

Notons que tous les objets connectés pour la santé ne sont pas considérés comme des dispositifs médicaux et ne sont pas tous de qualité certifiée. La HAS a publié fin 2016 un référentiel de 101 bonnes pratiques pour favoriser le développement d'applications et objets connectés sûrs, fiables et de qualité[98] et la mise en œuvre d'un référentiel de labellisation a été proposée en 2017 par le Comité stratégique de filière Santé. La HAS rappelle que les objets connectés considérés comme des dispositifs médicaux sont tenus de respecter le RGPD sur la protection des données personnelles[99]. Dans le cas de la COVID-19, cela concerne les données qui peuvent être recueillies par des oxymètres, par exemple.

Certains de ces objets connectés peuvent être utilisés par le patient seul, d'autres demandent l'aide d'un soignant, tel un infirmier. Certains d'entre eux peuvent aussi être utilisés hors du cadre d'une téléconsultation et transmettre les données collectées directement au médecin dans le but d'améliorer la prise en charge du patient, comme cela se fait déjà. Ces objets peuvent aussi être rassemblés dans une cabine de téléconsultation installée, par exemple, dans une pharmacie. Enfin, les objets connectés médicaux, par-delà le recueil et la transmission de données médicales, peuvent être enrichis de capacités algorithmiques permettant une aide au diagnostic.

Notons que tous les soignants et patients n'ont pas le même accès à ces objets connectés ni la même facilité d'utilisation, ce qui pose un problème d'équité.

<u>Points de vigilance :</u>

16. Garantir l'accessibilité des objets connectés de santé de qualité certifiée, proposer un accompagnement pour guider leur utilisation et assurer la protection des données issues de leur usage.

17. Veiller à la robustesse, la sécurité, la transparence, et la traçabilité des algorithmes liés aux objets connectés pour l'aide au diagnostic.

[98] https://www.has-sante.fr/jcms/c_2682685/fr/applis-sante-la-has-etablit-101-regles-de-bonne-pratique
[99] https://www.has-sante.fr/jcms/c_2905546/fr/evaluer-les-dispositifs-medicaux-connectes-y-compris-ceux-faisant-appel-a-l-intelligence-artificielle

Conclusion

L'augmentation significative de l'usage de la télémédecine témoigne, comme pour le téléenseignement ou le télétravail, de l'évolution majeure de nos manières de traiter et d'échanger des informations, constatée tout particulièrement dans le contexte de la crise provoquée par l'épidémie de SARS-Cov-2. L'accroissement du nombre de téléconsultations dès le début de l'épidémie et surtout pendant le confinement a révélé des enjeux d'éthique dans l'usage du numérique en télémédecine. Ce bulletin de veille montre à la fois l'intérêt et la complexité de la combinaison des exigences médicales et numériques en mettant en exergue plusieurs de ces enjeux et en alertant sur des points de vigilance permettant de les respecter.

Il conviendrait, à la sortie de cette crise sanitaire, de reprendre ces premiers points de vigilance dans le cadre d'une réflexion approfondie portant sur ces enjeux d'éthique. Au-delà de l'usage de la télémédecine pendant la crise, s'imposerait aussi une délibération la plus ouverte possible portant sur les conséquences humaines des pratiques médicales recourant à l'usage des objets numériques. Le CCNE a souligné à l'occasion des États généraux de la bioéthique en 2018 combien cette réflexion sur la place de l'humain dans le bouleversement du système de santé s'avérait centrale pour nos concitoyens[100]. La télémédecine, numérique par conception, transforme et potentiellement globalise mondialement les systèmes de santé, rendant nécessaire une réflexion collective aux niveaux national, européen et international sur les enjeux d'éthique de cette évolution.

[100] Rapport de synthèse du CCNE sur les états généraux de la bioéthique pp. 165 : https://www.ccne-ethique.fr/fr/actualites/le-rapport-des-etats-generaux-de-la-bioethique-2018-version-editee-est-en-ligne

Récapitulatif des points de vigilance

1. Proposer des formations aux pratiques professionnelles de télémédecine à destination des soignants, portant sur les aspects techniques et sur les spécificités de cette nouvelle pratique médicale.
2. Sensibiliser les soignants aux enjeux éthiques de l'usage des outils numériques.
3. Fournir une information explicite aux patients sur les modalités de la téléconsultation et les enjeux éthiques de ces outils numériques, et les accompagner dans l'accès et l'usage de ces outils.
4. Veiller à ce que, en dépit des contraintes liées à la situation d'urgence sanitaire et à l'utilisation de dispositifs de communication à distance, l'information et le recueil d'un consentement libre et éclairé du patient soient respectés. Une attention particulière concerne les données collectées et conservées, même temporairement, sur une plate-forme.
5. Sensibiliser l'ensemble des intervenants à l'importance de bien identifier les conditions et les finalités du traitement des données recueillies pendant une téléconsultation ou des télésoins (objectifs de recherche, par exemple) et de s'assurer de la qualité et du statut des prestataires associés (publics, privés, nationaux ou étrangers).
6. Veiller à ce que les patients opposés à la téléconsultation ne subissent ni discrimination, ni pénalisation sur le plan de la qualité de leur prise en charge médicale.
7. Les inégalités d'accès à la télémédecine constituent un véritable enjeu d'éthique, en particulier s'agissant des populations en situation de précarité. Des actions concrètes pourraient permettre de réduire ce préjudice par exemple en développant des espaces dédiés à la téléconsultation, comme dans les pharmacies ou autres lieux de proximité, et/ou en faisant appel à des intermédiaires de proximité habitués à l'usage des outils informatiques comme certaines administrations locales, les auxiliaires de soin ou les associations.
8. En toutes circonstances, utiliser des outils de communication de données de santé sécurisés respectant la réglementation relative à leur hébergement et leur traitement.
9. Dès à présent informer sur les outils numériques sécurisés de communication existants pour la télémédecine et s'assurer de leur appropriation par les professionnels de santé et la population.
10. Veiller à concevoir des systèmes d'information interopérables ainsi que des outils de communication et des centres d'hébergement et de traitement d'informations souverains et sécurisés pour la télémédecine et les évaluer régulièrement de manière indépendante.

11. Au-delà de l'urgence de la crise sanitaire, sensibiliser les citoyens aux risques associés au cheminement des données numériques et à l'exploitation des données collectées dans le cadre des téléconsultations à l'aide d'outils non sécurisés.

12. Une exigence d'éthique est d'éviter le développement non maîtrisé du marché de la santé afin de respecter le principe de solidarité nationale sur lequel est fondé notre système de soins et d'assurance maladie. En particulier il convient de s'assurer que les plates-formes de téléconsultation respectent les obligations déontologiques et réglementaires qui s'appliquent à la prise en charge médicale.

13. Soumettre à audit et validation les applications de questionnaires en ligne.

14. Lors d'un télésuivi par questionnaires numériques, garantir un contrôle interactif régulier entre le patient et un soignant.

15. Veiller à sensibiliser les utilisateurs aux risques de diagnostic erroné ou d'usage abusif de leurs données personnelles lorsqu'ils répondent à des questionnaires en ligne sur la santé sans la médiation d'un médecin.

16. Garantir l'accessibilité des objets connectés de santé de qualité certifiée, proposer un accompagnement pour guider leur utilisation et assurer la protection des données issues de leur usage.

17. Veiller à la robustesse, la sécurité, la transparence, et la traçabilité des algorithmes liés aux objets connectés pour l'aide au diagnostic.

Annexes

Personnes auditionnées

- **Frédéric Adnet,** chef du service des urgences de l'hôpital d'Avicenne et du SAMU de la Seine-Saint-Denis
- **Ghislaine Alajouanine,** présidente de l'Académie francophone de télémédecine
- **Myriam Burdin, Samuel Delafuys, Yann le Douarin**, Bureau « Coopérations et contractualisations » de la Direction générale de l'offre de soins, ministère des Solidarités et de la Santé.
- **Dominic Cliche,** conseiller en éthique **et Jocelyn Maclure,** président de la Commission de l'éthique en science et en technologie du Québec
- **Les médecins-chefs François Debrus,** pilote du projet de télémédecine pour la Direction de la médecine des forces et **Guillaume Martin**, responsable de conduite du projet Axone, Direction des services d'information et du numérique, Ministère des armées
- **Alexandre Falzon,** directeur général **et Guillaume Fayolle,** directeur général et co-fondateur**,** Nouveal e-santé, Covidom
- **Jacques Lucas,** président de l'Agence du numérique en santé
- **Andrea Reis**, co-directeur de l'Équipe d'éthique de la santé mondiale de la Division de la Scientifique en chef à l'OMS
- **Nathalie Salles**, présidente élue de la Société Française de Télémédecine
- **Jean-François Thébaut**, vice-président de la Fédération française des diabétiques

Constitution du groupe de travail

Membres du CNPEN - Membres du CCNE- Membres des deux comités***

Mounira Amor-Guéret*
Raja Chatila, co-rapporteur
Laure Coulombel**, co-rapporteure
Claude Delpuech*
Laurence Devillers
Karine Dognin-Sauze
Christine Froidevaux, co-rapporteure
David Gruson
Claude Kirchner**
Anne Pellé*
Francis Puech*

La publication de ce bulletin a été validée le 8 juillet 2020 lors de l'assemblée plénière incluant Emmanuel Didier (membre du CCNE) en tant qu'invité avec 14 voix pour et 2 abstentions.

ENJEUX D'ÉTHIQUE DU NUMÉRIQUE DU SUIVI ÉPIDEMIOLOGIQUE EN SORTIE DE CONFINEMENT

Communiqué de presse
Publié le 29 avril 2020

https://www.ccne-ethique.fr/fr/actualites/communique-du-comite-national-pilote-dethique-du-numerique

La sortie progressive du confinement va bientôt débuter en France. Elle se fait au risque, majeur, d'un rebond rapide de l'épidémie (dans quatre mois), voire très rapide (dans un mois). C'est ce que souligne l'avis du Conseil scientifique du 20 avril 2020 qui insiste sur les incertitudes de l'après-confinement dues à nos connaissances encore incomplètes sur le SARS-CoV-2. Un tel rebond provoquerait la résurgence d'un nombre important de décès, mais aussi le risque qu'une part significative de la population soit malade, avec de potentielles séquelles. Il aurait, en outre, un impact négatif sur la confiance des citoyens, sur l'éducation de la maternelle à l'université, sur l'emploi, sur l'économie, et plus généralement sur la prospérité de notre pays.

Ce risque d'une nouvelle vague épidémique faisant suite à l'arrêt du confinement peut être maîtrisé en mettant en place un suivi épidémiologique efficace en sortie de confinement. Il demande des moyens humains et techniques inédits, pour réaliser des centaines de milliers de tests par semaine, prendre en charge les personnes malades et retracer leurs contacts. Une détection aussi rapide et complète que possible est le seul moyen d'arrêter la chaîne de transmission en identifiant les personnes possiblement contaminées mais non encore symptomatiques, qui peuvent être des proches, des collègues de travail ou des inconnus croisés dans un lieu public ou privé. Pour permettre au système de santé français de réaliser ce suivi épidémiologique, le numérique sera d'une aide cruciale.

Ainsi, les équipes mobiles, qui selon l'avis du Conseil scientifique, pourraient être chargées du suivi des personnes infectées, devraient disposer d'un éventail d'outils numériques facilitant leur mission. Le suivi épidémiologique pourrait alors s'appuyer, d'une part, sur une application de suivi numérique de contacts pour les personnes en possession d'un smartphone et, d'autre part, sur des outils d'aide à la recherche de contacts pour les personnes qui n'auraient pas de smartphone ou auraient décidé de ne pas utiliser l'application qui serait proposée. On peut anticiper qu'un tel outil puisse contribuer [1] [2] au contrôle de la propagation de l'épidémie, dans le cadre d'une stratégie sanitaire globale et dans l'intérêt général. Les qualités éthiques requises d'une telle application ont fait l'objet du premier bulletin de veille du CNPEN [3] qui formule des recommandations portant en particulier sur la durée précise de sa mise en œuvre et l'information régulière, librement accessible, loyale et transparente sur la conception, le code, l'utilisation des moyens de suivi numérique, leur finalité et l'exploitation des données collectées. Par ailleurs, les enjeux éthiques des interactions de l'application de suivi numérique de

contacts avec les autres composantes du système de suivi épidémiologique devront être analysés précisément et soumis à un contrôle démocratique.

Le CNPEN attire l'attention sur le fait que plusieurs applications de suivi numérique de contacts pourraient être mises à disposition des utilisateurs de smartphones en France. L'absence de validation nationale d'une application de référence risquerait de se traduire par l'adoption de fait, par les utilisateurs, d'applications de suivi diverses, sans garanties éthiques ni contrôle démocratique, dont les objectifs, le code, la compatibilité et plus largement le fonctionnement, échapperaient au système de santé français, avec des conséquences incertaines sur leur efficacité sanitaire et le respect des libertés individuelles et collectives. C'est dans ce contexte qu'est développée à la demande du gouvernement, la proposition d'application de suivi numérique de contacts Stopcovid [4] qui bénéficie d'ores et déjà d'un avis constructif et de recommandations de la CNIL [5] et du CNNum [6] et plus récemment d'avis de l'ANSSI [7] et du CNCDH [8].

Le CNPEN, en coopération avec le CCNE [9], va travailler sur l'ensemble des enjeux éthiques du numérique qui se posent dans le cadre de la levée du confinement. Mais il souhaite insister sans délai sur l'importance que représente la mise en place d'une application de suivi numérique de contacts dont le contrôle souverain puisse être garanti aux citoyens français, voire européens, dès lors qu'il aura été statué sur ses qualités éthiques, en toute indépendance et transparence, pour le temps de la crise sanitaire mais aussi sur le long terme.

[1] https://www.research.ox.ac.uk/Article/2020-04-16-digital-contact-tracing-can-slow-or-even-stop-coronavirus-transmission-and-ease-us-out-of-lockdown
[2] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7144575/
[3] https://www.ccne-ethique.fr/fr/actualites/comite-national-pilote-dethique-du-numerique-bulletin-de-veille-ndeg1
[4] https://www.inria.fr/fr/stopcovid
[5] https://www.cnil.fr/fr/publication-de-lavis-de-la-cnil-sur-le-projet-dapplication-mobile-stopcovid
[6] https://cnnumerique.fr/StopCOVID-Avis
[7] https://www.ssi.gouv.fr/uploads/2020/04/anssi-communique_presse-20200427-application_stopcovid.pdf
[8] https://www.cncdh.fr/node/2069
[9] https://www.ccne-ethique.fr/fr/actualites/la-contribution-du-ccne-la-lutte-contre-covid-19-enjeux-ethiques-face-une-pandemie

ENJEUX D'ÉTHIQUE CONCERNANT DES OUTILS NUMÉRIQUES POUR LE DÉCONFINEMENT

Avis
Publié le 14 mai 2020

https://www.ccne-ethique.fr/fr/actualites/cnpen-enjeux-dethique-concernant-des-outils-numeriques-pour-le-deconfinement

Réponse à la saisine de messieurs

Olivier Véran

Ministre des Solidarités et de la Santé

Cédric O

Secrétaire d'État chargé du numérique

NOTE DE SYNTHÈSE

Les outils numériques peuvent être particulièrement utiles dans les différentes phases de déconfinement et au-delà. Leur intérêt doit être considéré par rapport au cadre global de la stratégie incluant les gestes barrières, les tests, le diagnostic, l'isolement, l'accompagnement, le traitement et l'hospitalisation.

Dans ce contexte, le Comité national pilote d'éthique du numérique (CNPEN) a été **saisi** par le ministre des Solidarités et de la Santé et le secrétaire d'État chargé du Numérique au sujet de *la conception, la mise en œuvre et les usages d'outils numériques* dans les différentes phases du déconfinement. **Cette note synthétise l'avis rendu suite à cette saisine.** Il souligne notamment que si ces outils peuvent accompagner la stratégie du gouvernement consistant à « **protéger, tester, isoler** », ils peuvent en outre aider à **anticiper** les évolutions et les conséquences de cette pandémie et à mieux prévenir de futures crises sanitaires.

Le comité livre donc un panorama d'outils numériques qu'il serait possible d'utiliser dans ce contexte, suivi d'une analyse des enjeux éthiques spécifiques aux applications de traçage numérique d'une part, et aux systèmes d'informations SI-DEP et Contact Covid d'autre part. Il tire de cette réflexion des recommandations et des points d'attention qui visent à accompagner la conception, la mise en œuvre et les usages de ces outils numériques.

Les proximités physiques de personnes révèlent potentiellement leurs relations sociales privées, associatives, professionnelles, politiques, ce sont donc des **informations personnelles particulièrement sensibles**. Ce sont aussi des **informations extrêmement utiles** pour permettre d'avertir d'un risque de contagion les personnes ayant côtoyé une personne infectée et donc d'aider à prévenir la propagation d'une épidémie. À l'échelle d'un pays ou d'un continent, des mesures permettant de détecter ces proximités, appelées traçages de contacts, ne peuvent être mises en œuvre que grâce à des outils numériques. Ceux-ci peuvent être soit des aides à des équipes sanitaires (comme SI-DEP et Contact Covid), soit des applications de traçage numérique (par exemple en utilisant des smartphones comme le propose StopCovid) soit encore leur combinaison éventuelle.

Le comité rappelle que tous les outils numériques qui aident au traçage des contacts d'une personne doivent répondre aux exigences formulées par les cadres réglementaires européen et français sur la protection des données personnelles. Il convient en ce sens de privilégier des moyens techniques favorisant la protection des données, de veiller au caractère proportionné de leur collecte et de définir les délais légaux de leur utilisation. Pour cela, il est nécessaire que les **autorités publiques** soient en mesure de **contrôler l'activation, l'adaptation des paramètres ou la désactivation** de ces outils en fonction de l'évolution de la situation sanitaire.

Par ailleurs, ces outils de traçage doivent constituer des mesures d'accompagnement et d'aide dans une stratégie plus globale. En ce sens, ils ne doivent pas engendrer des **discriminations** envers les personnes n'ayant pas accès à ces outils ou envers celles qui sont testées positives ou potentiellement contaminées. Leur déploiement doit se faire dans une logique démocratique, supposant une adhésion volontaire et un consentement libre et éclairé des utilisateurs, sans contrainte ni pression. Pour être garanti, un tel

consentement doit pouvoir s'appuyer sur **des informations régulières, transparentes, loyales et compréhensibles par tous**. Des mesures permettant à l'utilisateur de revenir sur son consentement, d'obtenir l'effacement ou la correction des données le concernant, doivent être anticipées. Le cadre de l'utilisation de ces outils doit pouvoir faire l'objet d'un débat public averti sur les enjeux techniques et sociétaux qu'elle soulève. À ce titre, le CNPEN recommande la **création d'un comité de suivi unique**, chargé d'identifier et de traiter les problèmes éthiques, juridiques et sociétaux posés par les différents outils de traçage dans le contexte de la stratégie de déconfinement.

Malgré le contexte d'urgence dans lequel ils sont déployés, des garanties doivent pouvoir être fournies quant à la **robustesse et à la sécurité** de ces outils. Des **expérimentations** sont donc indispensables et doivent être prolongées tout au long de leur déploiement et de leur utilisation. En outre, des audits doivent être conduits par des tiers de confiance. Le comité souligne par ailleurs qu'il est important de viser **l'interopérabilité** des différentes applications de traçage déployées aux niveaux national ou international. Enfin, la combinaison de différents systèmes d'information, notamment lorsque certains traitent des données anonymisées et d'autres traitent des données qui ne le sont pas, peut complexifier la garantie de la **confidentialité** et doit donc faire l'objet d'une vigilance particulière. **Les équipes sanitaires et les différents acteurs** utilisant les informations collectées par ces dispositifs doivent être **sensibilisés** à ces enjeux.

Cette réponse s'appuie sur le travail de veille relative aux questions éthiques soulevées par les usages du numérique dans la situation de crise créée par l'épidémie, entrepris par le CNPEN depuis le 19 mars. Elle s'inscrit donc dans la continuité d'un premier bulletin publié le 7 avril, portant en particulier sur le suivi des personnes par les outils numériques [1], et du communiqué sur le suivi épidémiologique en sortie de confinement publié le 29 avril [2].

[1] Réflexions et points d'alerte sur les enjeux d'éthique du numérique en situation de crise sanitaire aiguë

[2] Enjeux d'éthique du numérique du suivi épidémiologique en sortie de confinement.

ENJEUX D'ÉTHIQUE CONCERNANT DES OUTILS NUMÉRIQUES POUR LE DÉCONFINEMENT

I. Introduction

Le Comité national pilote d'éthique du numérique (CNPEN) a été saisi le 30 avril 2020 par le ministre des Solidarités et de la Santé et le secrétaire d'État chargé du Numérique au sujet *des questionnements éthiques liés à la conception, à la mise en œuvre et aux usages d'outils numériques* dans les différentes phases du déconfinement, en particulier en ce qui concerne *le respect de la vie privée et des libertés publiques* et les *effets structurants* que pourraient induire ces outils à moyen et long terme, notamment sur les citoyens et la société.

La réponse à cette saisine que constitue le présent avis a été élaborée dans des délais très courts compte tenu du contexte de rapidité dans lequel doivent être mises en œuvre les décisions du gouvernement. Cependant, le CNPEN avait mis en place dès le 19 mars un groupe de travail spécifique pour effectuer une veille relative aux questions éthiques soulevées par les usages du numérique dans la situation de crise créée par l'épidémie. Ceci a donné lieu à la publication le 7 avril d'un premier bulletin de *Réflexions et points d'alerte sur les enjeux d'éthique du numérique en situation de crise sanitaire aiguë*, avec en particulier un accent mis sur le *suivi des personnes par des outils numériques*, puis d'un communiqué le 29 avril relatif aux *Enjeux d'éthique du numérique du suivi épidémiologique en sortie de confinement*. Le présent avis s'appuie en particulier sur ces deux documents. Il a aussi été élaboré en coopération avec le CCNE pour les sciences de la vie et de la santé qui, pour sa part a été saisi le 4 mai par le Conseil scientifique Covid-19 sur les enjeux éthiques du déconfinement.

La situation de crise amorcée par la pandémie de la Covid-19 a conduit à une amplification inédite des usages du numérique ainsi qu'à la création de nouveaux outils. Ils sont devenus essentiels à tous les niveaux, d'un point de vue sociétal, économique et sanitaire, entraînant également une exacerbation de leurs enjeux éthiques.

Sur le plan sanitaire, les outils numériques peuvent notamment contribuer à identifier les transmissions possibles entre des porteurs du virus et des personnes avec lesquelles ils ont été en situation de proximité, ceci afin de faciliter une alerte rapide des porteurs potentiels. Au niveau collectif, ces outils permettent en particulier d'étudier et de modéliser l'évolution de l'épidémie, d'identifier d'éventuels nouveaux foyers, et de contribuer à l'évaluation de l'immunité de la population dans un contexte où les connaissances relatives à la pandémie sont encore partielles. Ils prennent tout leur sens et montrent leur utilité dans le cadre d'un dispositif global qui inclut les gestes barrières, les tests, le diagnostic, l'isolement, l'accompagnement, le traitement et l'hospitalisation.

Toutefois la conception, la mise en œuvre et l'utilisation de ces outils dans le contexte de la pandémie mettent en tension d'une part, les impératifs sanitaires avec le respect des libertés fondamentales et la protection de la vie privée et des données personnelles, et d'autre part, l'urgence de leur déploiement avec les questions de souveraineté, d'expérimentation, de contrôle, et d'information loyale du public.

Dans cet avis, nous présentons d'abord un panorama d'outils numériques qui pourraient être utilisés dans les différentes phases de déconfinement et au-delà. Nous nous focalisons ensuite sur l'analyse spécifique des enjeux d'éthique relatifs aux outils numériques de traçage des personnes susceptibles de propager le virus. Comme nous l'explicitons synthétiquement en annexe, ce traçage peut être réalisé de plusieurs manières, complémentaires, en s'appuyant à la fois sur des applications de traçage numérique et des équipes sanitaires qui recueillent et échangent des informations portant sur des personnes et sur leurs contacts sociaux. Nous analysons donc les questions d'éthique relatives aux applications de traçage numérique – et tout particulièrement celles qui reposent sur l'utilisation de techniques de type Bluetooth – puis celles qui sont relatives à leur utilisation combinée avec les systèmes d'information SI-DEP et Contact Covid prévus en soutien des équipes sanitaires, tels qu'ils sont en particulier décrits dans le Décret n° 2020-551 du 12 mai 2020[101]. De ces analyses nous tirons des points d'attention et des recommandations qui visent à éclairer la conception, la mise en œuvre et les usages de ces outils numériques.

---

[101] Décret n° 2020-551 du 12 mai 2020 relatif aux systèmes d'information mentionnés à l'article 11 de la loi n° 2020-546 du 11 mai 2020 prorogeant l'état d'urgence sanitaire et complétant ses dispositions

II. Les outils numériques dans le cadre de la crise Covid-19

La stratégie du gouvernement pour le déconfinement repose sur trois piliers : protéger, tester, isoler. Ces trois éléments nécessitent la mise en œuvre de moyens spécifiques à court, moyen et long termes, incluant des outils numériques variés. À titre d'exemples, des outils numériques pourraient aider à protéger les usagers des transports en commun en les informant sur l'affluence en temps réel ; à identifier les personnes à tester suite à leur contact rapproché avec des personnes infectées ; et permettre aux personnes susceptibles d'être infectées de continuer à communiquer ou d'être suivies médicalement tout en étant isolées. Par ailleurs, les outils numériques peuvent aussi contribuer, en particulier dans le cadre d'actions de recherche, à anticiper les évolutions et les conséquences de cette pandémie et à mieux prévenir de futures crises sanitaires.

Le tableau suivant présente des outils numériques qui sont utilisés, ou auxquels il serait possible de recourir, pendant les différentes phases de déconfinement et au-delà, en indiquant leurs usages en vue de **protéger (P), tester (T), isoler (I) et anticiper (A).**

Outils numériques	P	T	I	A
Applications de traçage de contacts		x	x	x
Systèmes d'information pour le recensement et le traçage de contacts par les équipes sanitaires (SI-DEP et Contact Covid)		x	x	x
Outils facilitant l'information des équipes sanitaires et leur interaction avec les personnes à tester ou à suivre		x	x	
Outils d'auto-diagnostic, outils pour la médecine de ville, télémédecine	x	x	x	
Outils d'information du public et d'expression citoyenne	x	x	x	x
Outils de modélisation pour le suivi et la prédiction de la propagation de l'épidémie	x			x
Outils d'analyse statistique de données et de prospective à long terme pour la recherche	x			x
Outils d'analyse et de visualisation pour l'imagerie médicale		x		x
Outils pour la recherche médicale (aide à la recherche de médicaments, de vaccins, etc.)	x			x
Robots pour les analyses médicales		x		

Outils numériques	P	T	I	A
Robots pour l'aide à la désinfection	x			
Robots d'aide à la livraison de repas, de médicaments	x			
Outils d'information et d'orientation des usagers des transports	x			
Contrôle automatique des autorisations d'accès aux transports	x			
Vidéosurveillance du respect des gestes barrières dans les lieux et transports publics	x			
Fabrication automatisée de produits critiques (masques, écrans protecteurs, embouts de respirateur, etc.)	x			
Outils permettant d'organiser et de poursuivre les activités économiques, sociales, éducatives et culturelles (télétravail, téléenseignement, etc.)	x		x	

Les outils numériques contribuent ainsi à concilier des objectifs sanitaires, économiques et sociaux. Toutefois leur conception, leur mise en œuvre et leur utilisation font apparaître certaines tensions éthiques. Elles sont exposées dans la suite de ce document pour ce qui concerne les applications et les systèmes d'information relatifs au traçage des contacts.

III. Enjeux éthiques des applications de traçage numérique pour le suivi épidémiologique

A. Introduction aux applications de traçage sur smartphone

En phase de déconfinement et plus généralement en cours d'épidémie due à une maladie particulièrement contagieuse, la réduction des chaînes de contamination est de toute première importance. Elle repose d'abord sur la prévention et la protection, notamment les gestes barrières. Elle repose aussi sur l'identification des personnes réellement infectées et donc sur des tests médicaux, et enfin, sur la prise de contact la plus rapide et efficace possible avec les personnes potentiellement contaminées. Le nombre moyen de personnes auxquelles un sujet malade transmet la maladie, appelé facteur de transmission R0, doit être inférieur à 1 pour que l'épidémie régresse. La valeur de ce facteur de transmission résulte de plusieurs paramètres, incluant la prévention et la protection mais aussi la rapidité de l'identification des personnes potentiellement contaminées. Cette identification dépend des situations de proximité entre deux personnes dont l'une est porteuse du virus et symptomatique. Ce « traçage des contacts » peut s'effectuer soit par l'intervention directe de personnes habilitées, soit en utilisant des applications numériques permettant notamment de détecter et de mémoriser

automatiquement la proximité de deux smartphones que l'on suppose être portés par deux personnes (voir annexe 1), ou encore en combinant les deux approches.

Les applications de traçage numérique constituent donc à la fois une opportunité de contribution à la diminution du facteur R0 et un risque de fuite des données personnelles des personnes qui utilisent ces applications. Pour réduire ce risque, des protocoles préservant l'anonymat et renforçant la sécurité des applications de traçage ont été conçus, dont la majorité appartient à deux grandes classes de protocoles qualifiés de « centralisés » et « décentralisés ». L'annexe 1 en expose les grands principes selon que les informations sont principalement gérées par un serveur centralisé ou qu'elles sont principalement gérées localement sur les smartphones.

En termes de cybersécurité, les risques concernent les données stockées aussi bien sur les smartphones que sur un serveur centralisé, ainsi que les communications entre les smartphones ou entre ceux-ci et un serveur central. La circulation des données sur les réseaux, dont internet, présente également un risque de fuite.

La mise en œuvre d'une application de traçage nécessite aussi de prendre en compte les éléments de son architecture matérielle et logicielle. Le serveur central et les réseaux devront ainsi être configurés de sorte à garantir une disponibilité et une continuité de service assurant les objectifs de sécurité et de fiabilité de l'application de traçage. Ils pourraient aussi intégrer des outils d'apprentissage d'informations relatives à la durée et à l'intensité des contacts.

L'analyse des tensions éthiques induites par les choix réalisés par les concepteurs d'une application de traçage numérique nécessite d'examiner synthétiquement les techniques actuellement disponibles.

La détection de proximité peut s'effectuer en utilisant soit des techniques de localisation utilisant le GPS, le wifi ou le réseau cellulaire, voire une combinaison de plusieurs d'entre elles, soit en utilisant un protocole de communication locale tel que Bluetooth Low Energy (BLE) entre deux dispositifs numériques. La plupart des protocoles proposés en Europe utilisent cette dernière solution, éventuellement combinée à de la localisation. Faire ce choix technique nécessite d'être attentif à ses conséquences en termes de fiabilité de la détection de proximité. Notamment, l'ignorance d'un contexte protecteur des contacts (par exemple, la présence d'un mur ou la proximité entre un malade et un médecin portant un équipement de protection) augmenterait le nombre de faux positifs. Par ailleurs, l'utilisation du Bluetooth BLE par une application de traçage numérique est sujette, pour certaines marques de smartphones, à des restrictions d'utilisation de la part du fabricant et du propriétaire du système d'exploitation. Ces derniers sont alors en position de décider de favoriser, ou non, la mise en place de cette application de traçage.

Analyse des tensions éthiques propres aux applications de traçage numérique

Les choix techniques et sociétaux opérés lors de la conception, la mise en œuvre et l'utilisation d'une application de traçage sont susceptibles d'exacerber des tensions entre différents principes et valeurs éthiques qu'il s'agit de recenser, d'analyser, et qui nécessitent des arbitrages.

Choix et usages d'une application

En automatisant le traçage des contacts, en particulier dans l'espace public et dans les transports, une application sur smartphone permet d'accélérer le signalement des nouveaux cas de personnes potentiellement contaminées. Elle contribue ainsi à la réduction du facteur R_0 et au ralentissement de la propagation de l'épidémie, grâce à un confinement et un suivi médical proposés à ces personnes. À plus long terme, elle peut également contribuer au développement d'études statistiques ou de modèles prédictifs à l'échelle nationale ou internationale. On peut en outre envisager l'utilisation d'applications similaires dans le cas d'autres crises sanitaires (par exemple les épidémies de grippe saisonnière). Cependant, on pourrait craindre la pérennisation de tels dispositifs de traçage des contacts dans la population, leur usage à d'autres fins que la gestion des crises sanitaires, voire l'accoutumance de la population au recours à de telles mesures légitimées par le contexte de la pandémie actuelle.

Pour prévenir le risque d'atteinte à la vie privée que constituerait une telle pérennisation, des garanties devront être données quant au caractère temporaire et proportionné de l'utilisation des données recueillies par l'application. Le déclenchement d'une application, sa suspension ou l'ajustement de ses paramètres (mesure de la distance, niveau d'alerte, …) devront être décidés par les autorités publiques compétentes sur la base de l'évolution sanitaire de la situation.

Le critère de proportionnalité implique que les applications minimisent le volume des données collectées et garantissent l'anonymat, afin que ni l'identité de la personne contaminée ni celle de ses contacts ne puissent être accessibles, y compris à l'application elle-même. Cependant, cette anonymisation peut rendre plus difficile la nécessaire prise en charge de la personne contaminée par les professionnels du soin.

En outre, si de tels outils de traçage se révélaient insuffisamment efficaces, d'autres techniques telles que la géolocalisation pourraient être envisagées, avec des risques éventuels d'atteinte à la vie privée.

Pour pouvoir maîtriser toutes ces dimensions, les autorités publiques doivent être en mesure de faire leurs propres choix d'application. Il est particulièrement important de recourir à des dispositifs numériques de traçage conçus et déployés avec un souci d'interopérabilité, notamment européenne et internationale. Le déploiement d'applications nationales non interopérables et la multiplication d'applications proposées par des acteurs privés et/ou internationaux susceptibles d'établir des listes de contacts différentes pourraient limiter l'efficacité du traçage numérique. Cette multiplicité pourrait également conduire à une limitation de la liberté de circulation, en particulier d'un pays à un autre.

Recommandations :

3.1 Viser l'interopérabilité des applications de traçage, au niveau européen, voire international, dans le respect du RGPD[102].

3.2 Veiller à la non-discrimination des personnes qui n'utilisent pas les applications volontaires de traçage, y compris dans le contexte de déplacements en Europe et à l'international.

3.3 Choisir des moyens techniques de détection de proximité qui favorisent la protection de la vie privée et des données personnelles.

3.4 Donner la possibilité aux autorités publiques compétentes d'activer ou de désactiver les applications de traçage qui ont été volontairement installées par leurs utilisateurs en en informant ces derniers.

3.5 Donner à tout moment la possibilité aux utilisateurs qui ont volontairement installé une application de traçage sur leur smartphone de la désactiver temporairement ou de la désinstaller définitivement.

3.6 Prévoir la désactivation automatique des applications de traçage après l'expiration de leur délai légal ainsi que les moyens d'en rendre compte publiquement.

Transparence

L'efficacité d'une application dépend en particulier de l'adhésion de la population à son utilisation, qui repose sur la confiance accordée à l'ensemble du dispositif de prévention et de soin mis en place. Cette adhésion ne peut se faire sans une information régulière, librement accessible, loyale et transparente. Cette information doit concerner la conception et le code de l'application, y compris leurs auteurs, la finalité de l'application ainsi que l'exploitation des données qu'elle collecte, afin que chacun puisse être assuré qu'elle ne fait que ce qu'elle est censée faire. En particulier, la publication du code source de l'application est une condition élémentaire de transparence. La loyauté de l'information suppose en outre que les termes employés pour décrire les aspects techniques ne soient pas ambigus et apportent effectivement des éléments de compréhension pour tous. Par exemple, l'utilisation des termes « centralisé » et « décentralisé », qui sont chargés de sens implicites, peut brouiller la compréhension des dispositifs techniques.

Cette information, complétée de données relatives notamment au taux de diffusion des applications dans la population et de résultats d'audits réalisés au niveau national par des tiers de confiance, doit permettre de nourrir les contrôles institutionnels et démocratiques ainsi que les débats publics.

[102] Règlement général européen sur la protection des données

Recommandations :

3.7 Garantir l'information régulière, librement accessible, loyale et transparente sur la conception et le code des applications de traçage, leur finalité ainsi que sur l'exploitation des données qu'elles collectent. Veiller à ce que cette information comporte des éléments de compréhension pour tous.

3.8 Prévoir un cadre législatif et réglementaire afin d'organiser les contrôles institutionnels et démocratiques des applications de traçage et faciliter le débat public.

3.9 Soumettre les applications de traçage à l'audit par des tiers de confiance.

Consentement

Une application de traçage est conçue comme un dispositif permettant d'informer chacun d'un contact avec une personne contaminée et ainsi d'être acteur de sa propre santé et de celle des autres. Le caractère volontaire et non contraignant de son adoption peut néanmoins réduire son efficacité. Il faut aussi tenir compte du possible manque de réactivité de ces personnes ou de leur possible réticence à se soumettre à un test médical.

Malgré l'impact potentiellement négatif du volontariat sur l'efficacité du dispositif, celui-ci est indispensable et doit se fonder sur un consentement libre et éclairé. Cela suppose que le refus de consentir n'expose pas la personne à des conséquences négatives, quelle qu'en soit la nature.

Ce consentement repose sur la transparence et suppose la mise en place préalable d'une politique d'information et d'acculturation des citoyens, malgré le contexte d'urgence. Cette information doit en particulier exposer les implications et les limites de l'application, en particulier pour prévenir l'illusion d'être « protégé » par son smartphone et les comportements à risque qui en résulteraient. Par ailleurs, le consentement à l'utilisation de l'application et la responsabilisation des personnes mineures ou vulnérables doivent être questionnés et faire l'objet d'un accompagnement et d'une information adaptée. Une attention particulière doit être accordée aux personnes en situation de précarité sociale, ne maîtrisant pas la langue française ou à celles qui ne pourraient pas accéder à la technologie.

Si des politiques incitatives pour l'utilisation d'une application de traçage numérique étaient mises en place, elles devraient exclure tout système susceptible d'induire des biais et de provoquer la discrimination de certaines populations, en particulier les systèmes de récompense aux usagers.

On ne saurait écarter l'éventualité de la stigmatisation ou de formes éventuelles de pression envers les personnes qui n'utilisent pas d'application, notamment par les employeurs ou les assureurs. La possession d'un smartphone et l'utilisation d'une application ne peuvent aucunement constituer des conditions d'accès à des services ou des ressources, en particulier l'accès au soin et à l'emploi. Des mesures spécifiques et gratuites doivent être prévues pour les personnes qui ne disposent pas de smartphone mais qui souhaitent participer au dispositif de traçage.

Recommandations :

3.10 Rendre disponibles et accessibles à tous les publics des informations claires et loyales relatives aux objectifs, au fonctionnement et aux limites des applications de traçage. Ces informations devront être fournies sur un site de référence national en ligne, par téléphone, sous forme de documents imprimés et sous forme radio et télé diffusée.

3.11 Déployer une pédagogie large et adaptée à toute la population sur les enjeux techniques et sociétaux de ces applications de traçage.

3.12 Garantir le consentement libre et éclairé tout comme la possibilité de ne pas consentir et ceci sans pression, contrainte, ni mise en place de système de récompense.

3.13 Permettre aux personnes de revenir à tout moment sur leur engagement et permettre l'effacement des données collectées.

3.14 Prévoir des mesures spécifiques et gratuites pour les personnes ne disposant pas de smartphone et souhaitant participer au dispositif de traçage.

Point d'attention :

3.a L'utilisation d'une application de traçage doit faire l'objet d'une codécision entre les titulaires de l'autorité parentale et le mineur de moins de 15 ans.

Expérimentation

Pour pouvoir disposer d'une application de traçage robuste et fonctionnelle, il est nécessaire de l'expérimenter au préalable et ce, en toute transparence. Pour cela, il est préférable d'agir d'abord à petite échelle, sur un échantillon de population, avant le déploiement général. Une validation insuffisante ou une expérimentation précipitée de l'application pourraient nuire à son efficacité. Par exemple, cela pourrait induire un débordement inutile du système de tests médicaux par des faux positifs (notifiés mais testés négativement par la suite). Si une application de traçage connaissait des dysfonctionnements ou se révélait inefficace, la responsabilité et la réputation des entités l'ayant commanditée, conçue ou mise en œuvre pourraient être engagées, affectant ainsi la confiance dans la gestion de la crise.

Ces expérimentations se heurtent à deux limites : d'une part le choix et la taille de l'échantillon, et d'autre part le temps nécessaire pour les conduire. Si une application est déployée, il serait donc souhaitable, pour pouvoir la corriger et l'améliorer, de poursuivre les expérimentations durant le déploiement afin de prendre en compte leurs résultats en même temps que les retours d'expérience de ce déploiement.

Recommandation :

3.15 Si une application de traçage est déployée, mener des expérimentations même si sa mise en service doit intervenir rapidement. Poursuivre ces expérimentations en parallèle de son déploiement.

IV. Enjeux éthiques des interactions entre le traçage numérique et les systèmes d'information SI-DEP et Contact Covid pour le recensement et le traçage de contacts

La stratégie nationale de sortie du confinement s'appuie actuellement sur deux outils numériques[103] : SI-DEP (Système d'Information de Dépistage), un collecteur automatisé de résultats de tests diagnostiques (RT-PCR) qui permet de recenser les cas positifs, et Contact Covid, une base de données spécifique qui enregistre les patients testés positifs ainsi que leurs contacts rapprochés à des fins de suivi.[104]

Nous analysons ici les liens avérés ou potentiels entre les trois systèmes d'information que constituent SI-DEP, Contact Covid et une éventuelle application de traçage numérique. Notons d'abord que des données de SI-DEP, dont l'identité des personnes testées positives, sont traitées par Contact Covid[105]. Notons aussi qu'une application de traçage numérique enregistre tous les contacts indépendamment de leur signification, alors que SI-DEP et Contact Covid enregistrent uniquement les contacts suspicieux car le processus est déclenché par un médecin suite à un test médical ou à la présence de symptômes. Cela modifie l'évaluation de la proportionnalité et, en conséquence, les exigences d'anonymat que nous abordons ci-dessous.

Usages des systèmes d'information

Les membres des équipes sanitaires utilisateurs de SI-DEP et Contact Covid peuvent à la fois interpréter les données recueillies en contexte et expliquer les mesures sanitaires préconisées à la personne concernée ainsi qu'à ses contacts. Ceci est toutefois conditionné par le fait que ces utilisateurs des systèmes d'information soient assermentés et compétents.

Un questionnement relatif aux mesures de déconfinement opposerait l'efficacité d'une application de traçage numérique à celle des actions réalisées par des humains, notamment par les équipes sanitaires. Cette opposition conduit souvent à craindre des actions réalisées par des machines, même si elles sont peu intrusives, et à leur préférer des actions réalisées par des humains, même si elles sont plus intrusives. D'un côté, une base de données gérée par des opérateurs humains peut comporter autant, voire plus, de risques de rupture de la confidentialité que les données rassemblées par une application numérique. De l'autre côté, l'anonymat, qui est visé dans une application de traçage, ne permet pas l'accompagnement par des professionnels des personnes notifiées par l'application comme ayant été en contact avec des personnes testées positivement, du moins avant qu'elles ne se signalent elles-mêmes à leur médecin ou à une autorité de santé.

D'autres outils numériques pourraient aussi venir en soutien à l'intervention humaine à des fins de traçage. Par exemple, dans la démarche Contact Covid, la personne à laquelle il est demandé de signaler ses contacts pourrait s'appuyer le cas échéant sur l'historique

[103] LOI n° 2020-546 du 11 mai 2020 prorogeant l'état d'urgence sanitaire et complétant ses dispositions
[104] Voir le site du ministère des Solidarités et de la Santé, consulté le 11 mai 2020 à 11h.
[105] Décret n° 2020-551 du 12 mai 2020 relatif aux systèmes d'information mentionnés à l'article 11 de la loi n° 2020-546 du 11 mai 2020 prorogeant l'état d'urgence sanitaire et complétant ses dispositions

de géolocalisation de son propre téléphone, voire autoriser l'agent qui l'interroge à accéder à cet historique ou à son agenda. D'autres moyens numériques pourraient, en soutien à l'intervention humaine, aider à la priorisation des appels en fonction de la fréquence de contacts ou des zones les plus atteintes, ou offrir des outils d'interaction incluant le diagnostic via les outils de télémédecine. Ces outils soulèvent également des questions de confidentialité des données personnelles.

Par ailleurs, la procédure en plusieurs étapes de Contact Covid comporte des faiblesses potentielles. Elle repose d'abord sur les appels téléphoniques, avec le risque de ne pouvoir joindre les personnes concernées. Elle repose ensuite sur un entretien avec ces personnes, dont la mémoire n'est pas certaine ou qui ne souhaiteraient pas divulguer certaines informations. En conséquence, la base de données Contact Covid est potentiellement lacunaire et incorrecte. De plus, elle peut être biaisée par des actes de malveillance, par exemple la fausse déclaration de contacts. À l'inverse, un protocole formalisé automatique donnerait rapidement la liste exhaustive des contacts de la personne testée positive. En ce qui concerne ces aspects, le recours à une application de traçage numérique pourrait compléter et renforcer utilement la procédure Contact Covid.

La complémentarité entre une application de traçage et les systèmes d'information SI-DEP et Contact Covid pourrait donc permettre une détection plus rapide, plus rigoureuse et plus robuste des cas contacts. Leur mise en relation élargirait la possibilité de suivi individuel des personnes potentiellement contaminées. Cependant, la combinaison de ces deux types d'approches peut présenter deux risques majeurs. Un croisement de deux bases de données, l'une comportant des données anonymes et l'autre non (celle de l'application et celle des systèmes SIDEP et Contact Covid), peut conduire à perdre le caractère anonyme de la première. Par ailleurs, le caractère souverain[106] d'outils numériques tels que SI-DEP et Contact Covid pourrait être compromis par leur combinaison avec une application de traçage qui échappe au contrôle des autorités nationales.

<u>Recommandations :</u>

4.1 Veiller à maintenir le caractère anonyme d'une base de contacts constituée automatiquement par une application numérique dans le cas de sa mise en relation avec des systèmes d'information alimentés par des professionnels assermentés et dans lesquels les informations ne sont pas anonymisées.

4.2 Veiller à ce que la combinaison éventuelle des outils SI-DEP et Contact Covid avec une application de traçage n'échappe pas au contrôle des autorités nationales.

[106] La souveraineté permet d'être responsable de ses choix éthiques ; voir le rapport de la CERNA, *La souveraineté à l'ère du numérique Rester maîtres de nos choix et de nos valeurs*, Allistene, oct. 2018 ; http://cerna-ethics-allistene.org/digitalAssets/55/55708_AvisSouverainete-CERNA-2018.pdf

Point d'attention :

4.a Le croisement des deux bases de données SI-DEP et Contact Covid rend les informations de santé hautement identifiantes.

Le recours à des collaborateurs nouveaux, formés rapidement, ainsi que l'ouverture éventuelle des données médicales sensibles (état de santé de la personne, ses antécédents et ses traitements éventuels) à des acteurs qui n'y ont pas accès en conditions normales, sont susceptibles d'augmenter le risque de rupture du secret médical. La responsabilité de l'État et des divers acteurs impliqués serait engagée en cas de fuite de données ou de détournement d'usage.

Recommandation :

4.3 Former les membres des équipes sanitaires et les sensibiliser aux enjeux de la protection des données personnelles, notamment dans le contexte d'usage d'outils numériques. Veiller en particulier à la préservation du secret médical.

Anonymisation et pseudonymisation

Les données de santé nominatives contenues dans SI-DEP et Contact Covid sont pseudonymisées pour leur utilisation à des fins d'études épidémiologiques et de recherche.

De nombreuses études informatiques ont montré que la suppression de certaines données identifiantes, en particulier des noms et prénoms, éventuellement en les remplaçant par des pseudonymes, ne constitue pas une anonymisation au sens du RGPD. En effet, il existe un risque de ré-identification par croisement avec d'autres bases de données où figureraient explicitement des informations nominatives. Il convient donc d'être attentif à distinguer données « pseudonymisées » et données « anonymisées ».

Point d'attention :

4.b Des données de santé « pseudonymisées » ne sont pas des données « anonymisées », et doivent donc être considérées comme des données personnelles à protéger selon les principes imposés par le RGPD.

Protéger sans discriminer

Les données collectées par les équipes sanitaires ou par une application numérique sont des données sensibles qui pourraient être utilisées à des fins discriminatoires. Le Conseil de l'Europe souligne que « *le profilage ne doit pas entraîner de mesures discriminatoires d'aucune sorte* » en particulier sur les aspects politique, socio-économique, sexuel ou religieux[107]. De même l'OMS alerte sur le risque de stigmatisation des personnes présentant des caractéristiques perçues comme liées à la maladie[108].

Recommandation :

4.4 S'assurer de la non-discrimination des personnes testées positives, ainsi que des groupes qui pourraient être identifiés dans les analyses épidémiologiques, tout en leur appliquant les mesures d'isolement requises pour limiter la propagation de l'épidémie.

[107] Conseil de l'Europe "Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel", Série des Traités Européens n° 108, 1981
[108] Article 3 du Règlement Sanitaire International de l'OMS - 2005

V. Recommandations générales concernant les outils numériques de traçage

Pour la conception

5.1 Organiser des vérifications et des tests techniques tout au long du cycle de vie des outils numériques de traçage pour en évaluer la robustesse et la sécurité.

5.2 Faire évaluer l'efficacité des outils numériques de traçage par un organisme indépendant.

Point d'attention :

5.a À toutes les étapes de la conception et pour tous les composants techniques, veiller à respecter les cadres réglementaires français et européens, notamment le RGPD.

Pour la mise en œuvre

5.3 Définir et annoncer, pour chaque outil de traçage, une durée légale de son utilisation et de conservation des données traitées qui soit limitée et proportionnée à la durée de la pandémie. Documenter les conditions de la réversibilité de la mise en œuvre de ces outils.

5.4 Prévoir les moyens techniques et juridiques adaptés pour garantir la cybersécurité des outils numériques de traçage au vu de leur caractère intrusif et de leur usage massif.

5.5 Créer un comité de suivi unique et opérationnel pour identifier et traiter les problèmes éthiques, juridiques et sociétaux posés par les différents outils de traçage dans le contexte de la stratégie de déconfinement. Ce comité impliquera notamment des professionnels du numérique, de la santé, des sciences humaines et sociales ainsi que des parlementaires et des représentants de la société civile. Ce comité devrait s'articuler avec le Comité de contrôle et de liaison covid-19 instauré par la loi du 11 mai 2020 (art 11 VIII) chargé « *d'associer la société civile et le Parlement aux opérations de lutte contre la propagation de l'épidémie par suivi des contacts ainsi qu'au déploiement des systèmes d'information prévus à cet effet* ».

Pour les usages

5.6 Permettre aux personnes d'accéder aux données qui les concernent, de signaler une erreur, de demander une modification, de recevoir une réponse à leur requête dans un délai spécifié et d'initier un recours en cas de préjudice subi.

VI. Récapitulatif des recommandations générales et spécifiques :

Pour la conception

3.1 Viser l'interopérabilité des applications de traçage, au niveau européen, voire international, dans le respect du RGPD.

3.3 Choisir des moyens techniques de détection de proximité qui favorisent la protection de la vie privée et des données personnelles.

3.4 Donner la possibilité aux autorités publiques compétentes d'activer ou de désactiver les applications de traçage qui ont été volontairement installées par leurs utilisateurs en en informant ces derniers.

3.5 Donner à tout moment la possibilité aux utilisateurs qui ont volontairement installé une application de traçage sur leur smartphone de la désactiver temporairement ou de la désinstaller définitivement.

3.6 Prévoir la désactivation automatique des applications de traçage après l'expiration de leur délai légal ainsi que les moyens d'en rendre compte publiquement.

3.7 Garantir l'information régulière, librement accessible, loyale et transparente sur la conception et le code des applications de traçage, leur finalité ainsi que sur l'exploitation des données qu'elles collectent. Veiller à ce que cette information comporte des éléments de compréhension pour tous.

3.9 Soumettre les applications de traçage à l'audit par des tiers de confiance.

3.15 Si une application de traçage est déployée, mener des expérimentations même si sa mise en service doit intervenir rapidement. Poursuivre ces expérimentations en parallèle de son déploiement.

5.1 Organiser des vérifications et des tests techniques tout au long du cycle de vie des outils numériques de traçage pour en évaluer la robustesse et la sécurité.

5.2 Faire évaluer l'efficacité des outils numériques de traçage par un organisme indépendant.

Point d'attention :

5.a À toutes les étapes de la conception et pour tous les composants techniques, veiller à respecter les cadres réglementaires français et européens, notamment le RGPD.

Pour la mise en œuvre

3.8 Prévoir un cadre législatif et réglementaire afin d'organiser les contrôles institutionnels et démocratiques des applications de traçage et faciliter le débat public.

3.10 Rendre disponibles et accessibles à tous les publics des informations claires et loyales relatives aux objectifs, au fonctionnement et aux limites des applications de traçage. Ces informations devront être fournies sur un site de référence national en ligne, par téléphone, sous forme de documents imprimés et sous forme radio et télé diffusée.

3.11 Déployer une pédagogie large et adaptée à toute la population sur les enjeux techniques et sociétaux de ces applications de traçage.

3.12 Garantir le consentement libre et éclairé tout comme la possibilité de ne pas consentir et ceci sans pression, contrainte, ni mise en place de système de récompense.

4.1 Veiller à maintenir le caractère anonyme d'une base de contacts constituée automatiquement par une application numérique dans le cas de sa mise en relation avec des systèmes d'information alimentés par des professionnels assermentés et dans lesquels les informations ne sont pas anonymisées.

4.2 Veiller à ce que la combinaison éventuelle des outils SI-DEP et Contact Covid avec une application de traçage n'échappe pas au contrôle des autorités nationales.

4.4 S'assurer de la non-discrimination des personnes testées positives, ainsi que des groupes qui pourraient être identifiés dans les analyses épidémiologiques, tout en leur appliquant les mesures d'isolement requises pour limiter la propagation de l'épidémie.

5.3 Définir et annoncer, pour chaque outil de traçage, une durée légale de son utilisation et de conservation des données traitées qui soit limitée et proportionnée à la durée de la pandémie. Documenter les conditions de la réversibilité de la mise en œuvre de ces outils.

5.4 Prévoir les moyens techniques et juridiques adaptés pour garantir la cybersécurité des outils numériques de traçage au vu de leur caractère intrusif et de leur usage massif.

5.5 Créer un comité de suivi unique et opérationnel pour identifier et traiter les problèmes éthiques, juridiques et sociétaux posés par les différents outils de traçage dans le contexte de la stratégie de déconfinement. Ce comité impliquera notamment des professionnels du numérique, de la santé, des sciences humaines et sociales ainsi que des parlementaires et des représentants de la société civile. Ce comité devrait s'articuler avec le Comité de contrôle et de liaison covid-19 instauré par la loi du 11 mai 2020 (art 11 VIII) chargé « *d'associer la société civile et le Parlement aux opérations de lutte contre la propagation de l'épidémie par suivi des contacts ainsi qu'au déploiement des systèmes d'information prévus à cet effet* ».

Points d'attention :

4.a Le croisement des deux bases de données SI-DEP et Contact Covid rend les informations de santé hautement identifiantes.

4.b Des données de santé « pseudonymisées » ne sont pas des données « anonymisées », et doivent donc être considérées comme des données personnelles à protéger selon les principes imposés par le RGPD.

Pour les usages

3.2 Veiller à la non-discrimination des personnes qui n'utilisent pas les applications volontaires de traçage, y compris dans le contexte de déplacements en Europe et à l'international.

3.13 Permettre aux personnes de revenir à tout moment sur leur engagement et permettre l'effacement des données collectées.

3.14 Prévoir des mesures spécifiques et gratuites pour les personnes ne disposant pas de smartphone et souhaitant participer au dispositif de traçage.

4.3 Former les membres des équipes sanitaires et les sensibiliser aux enjeux de la protection des données personnelles, notamment dans le contexte d'usage d'outils numériques. Veiller en particulier à la préservation du secret médical.

5.6 Permettre aux personnes d'accéder aux données qui les concernent, de signaler une erreur, de demander une modification, de recevoir une réponse à leur requête dans un délai spécifié et d'initier un recours en cas de préjudice subi.

Point d'attention :

3.a L'utilisation d'une application de traçage doit faire l'objet d'une codécision entre les titulaires de l'autorité parentale et le mineur de moins de 15 ans.

Annexe 1 : Les différentes méthodes de suivi des contacts[109]

Dans un contexte sanitaire épidémique, imaginons qu'Alice et Bob se rencontrent et que, trois jours plus tard, il s'avère que Alice est malade. Comment peut-elle prévenir Bob, pour qu'il s'isole, se fasse tester et interrompe ainsi la chaîne de contamination ?

Un premier algorithme consiste, pour Alice, à noter dans un carnet le numéro de téléphone de Bob, ainsi que celui de toutes les personnes qu'elle a rencontrées, pour pouvoir les prévenir si jamais elle tombe malade. Mais Bob n'a pas nécessairement envie de donner son numéro à Alice, qui pourrait en faire un usage que Bob ne souhaite pas. Et s'il refuse de le donner ou s'il n'a pas de téléphone, il ne sera pas prévenu si Alice tombe malade.

Cette méthode – appelons-la Carnet Contact – oblige à déclarer son identité à toutes les personnes que l'on rencontre. Elle est intrusive et potentiellement peu efficace car Bob peut ne pas souhaiter donner ses coordonnées à Alice. C'est le principe de cette méthode qui est repris par les médecins pour éviter les épidémies très violentes, comme celles de méningite : quand une personne tombe malade, un enquêteur professionnel cherche à identifier toutes les personnes avec qui elle a été en contact, pour les diagnostiquer et leur proposer éventuellement des soins. Dans le cadre de la crise sanitaire de la Covid-19, c'est le principe du protocole réalisé via le système d'information Contact Covid[110].

Pour éviter cet algorithme intrusif de par son accès à l'identité des personnes, les informaticiens en ont inventé d'autres, plus respectueux de la vie privée et des données personnelles. Par exemple, quand Alice et Bob se rencontrent, ils sont désignés par des pseudonymes – par exemple Xlthlx et Qfwfq. Une tierce personne, Zoé, reçoit alors l'information que Xlthlx et Qfwfq se sont rencontrés. Quand Alice tombe malade, elle indique à Zoé que la personne « Xlthlx » est malade ; Zoé en déduit que la personne « Qfwfq » a été en contact avec une personne contaminée. Bob, tous les jours, demande à Zoé si la personne « Qfwfq » a été en contact avec une personne contaminée ; le troisième jour, Zoé lui répond par l'affirmative. Il en déduit l'existence de risque pour lui-même. Cette méthode, dans laquelle Zoé enregistre toutes les paires de pseudonymes à l'échelle d'un pays ou d'un continent, est dite « centralisée ». C'est la base du protocole ROBERT[111], qui est utilisé en particulier dans l'application de traçage StopCovid[112].

Mais il est aussi possible de procéder autrement. Une autre méthode, à la base du protocole DP3T[113], utilisée par exemple dans les applications de traçage favorisées par les propriétaires des systèmes d'exploitation, sera déployée notamment en Allemagne et en Suisse. Elle fonctionne sur le principe suivant. Bob note dans son téléphone qu'il a été en contact avec une personne dont le pseudonyme est Xlthlx ; puis, Alice prévient tous les téléphones utilisant ce protocole que la personne « Xlthlx » est malade, afin que Bob, parmi d'autres, sache qu'il a été en contact avec une personne contaminée. Cette méthode, dite « décentralisée » puisque Zoé n'y joue plus aucun rôle, demande de rendre publiques beaucoup d'informations. En effet, tous les téléphones qui l'utilisent contiennent

[109] D'après un article à paraître dans Pour la Science en juillet 2020.
[110] Voir le site du ministère des Solidarités et de la Santé
[111] https://github.com/ROBERT-proximity-tracing/
[112] https://gitlab.inria.fr/stopcovid19/accueil
[113] https://github.com/DP-3T/

l'information que la personne « XIthIx » est contaminée, alors que cette information n'est connue que d'Alice et de Zoé dans l'algorithme dit « centralisé ».

Dans le cas des protocoles dits « centralisés » ou « décentralisés », Alice peut prévenir Bob qu'elle est tombée malade depuis leur rencontre, sans que Bob n'ait besoin de communiquer à Alice, ni à personne, son numéro de téléphone ou son nom. Ces protocoles sont donc moins intrusifs que Carnet Contact. On peut aussi noter que, dans tous les cas, des attaques sont possibles, par exemple en dérobant le carnet d'adresses d'Alice dans le cas du protocole Carnet Contact, ou en menant une cyber-attaque dans le cas des deux autres types de protocoles.

Un troisième type de protocoles, qui associe des identifiants chiffrés uniques à chaque rencontre et non à chaque téléphone, est en cours de développement. Il pourrait ouvrir une troisième voie qui ne se limiterait pas au choix entre des protocoles dit centralisé ou décentralisé.[114]

[114] https://github.com/3rd-ways-for-EU-exposure-notification/project-DESIRE, mis en ligne le 9 mai 2020

Annexe 2 : Saisine

GOUVERNEMENT
Liberté
Égalité
Fraternité

Les Ministres

Paris, le 30 AVR. 2020

Monsieur le Directeur,

La stratégie de déconfinement, qui a été présentée le 28 avril 2020 par le Premier Ministre devant l'Assemblée nationale, repose sur trois piliers : protéger, tester et isoler. La mise en œuvre de cette stratégie va mobiliser de nombreux outils numériques qu'ils soient existants, et dont l'usage va être élargi, ou qu'ils constituent de nouveaux instruments en cours de développement.

Ces outils numériques sont mis en place dans un contexte d'urgence afin d'être disponibles rapidement dans les différentes phases de déconfinement. Néanmoins, le Gouvernement est particulièrement attaché à ce que ces outils respectent pleinement la vie privée de nos concitoyens et les libertés publiques. Au-delà de ces exigences, l'analyse de votre comité sur les enjeux éthiques de la mise en place de ces outils répondant à une nécessité impérieuse dans un contexte de crise mais également susceptibles d'avoir des effets structurants à moyen/long terme, permettrait d'éclairer les choix du Gouvernement.

Dans ce contexte, nous souhaiterions que le comité d'éthique du numérique puisse examiner les questionnements éthiques liés à la conception, la mise en œuvre, l'usage de ces outils afin que les réflexions qu'il pourra formuler puissent éclairer les travaux des semaines à venir mais aussi les débats sur l'utilisation de ces outils. Il serait particulièrement utile que le Comité pilote d'éthique du numérique nous transmette un avis d'ici au 11 mai.

Nous vous prions d'agréer, Monsieur le Directeur, l'expression de notre considération distinguée.

Olivier VERAN
Ministre des Solidarités et de la Santé

Cédric O
Secrétaire d'Etat
chargé du Numérique

Monsieur Claude KIRCHNER
Directeur du Comité national pilote d'éthique du numérique
Membre du CCNE
66 rue de Bellechasse
75007 PARIS

Personnes auditionnées

Franck Chauvin, Président du Haut Conseil de la santé publique et membre du Conseil Scientifique Covid-19
Marc Debrincat, Bruno Gazeau, Anne-Marie Ghermard de la Fédération Nationale des Associations d'Usagers des Transports
Luciano Floridi, professeur à l'université d'Oxford, membre du *Ethics Advisory Board for NHSx COVID-19 app*
Hélène Gebel, coordinatrice de l'espace de réflexion éthique du Grand Est et de la Conférence Nationale de Espaces de Réflexion Éthique Régionaux
Bruno Sportisse, Président-directeur général d'Inria

Composition du groupe de travail ayant contribué à l'élaboration de ce document

Gilles Adda
Raja Chatila
Theodore Christakis
Laure Coulombel
Camille Darche – rédactrice
Laurence Devillers
Emmanuel Didier
Karine Dognin-Sauze
Gilles Dowek
Valeria Faure-Muntian
Christine Froidevaux – co-rapporteuse
Jean-Gabriel Ganascia
Eric Germain
Alexei Grinbaum
David Gruson
Jeany Jean-Baptiste
Claude Kirchner
Caroline Martin
Tristan Nitot
Jérôme Perrin
Catherine Tessier – co-rapporteuse
Serena Villata
Célia Zolynski

CONSULTATION DE LA COMISSION EUROPÉENNE

LIVRE BLANC INTELLIGENCE ARTIFICIELLE. UNE APPROCHE EUROPEENNE

Contribution du Comité national pilote d'éthique du numérique

Publié le 15 juin 2020

https://www.ccne-ethique.fr/fr/actualites/contribution-du-cnpen-dans-le-cadre-de-la-consultation-sur-le-livre-blanc-de-la

Introduction

Le Comité national pilote d'éthique du numérique (CNPEN) a été mis en place en décembre 2019 sous l'égide du Comité consultatif national d'éthique (CCNE) à la demande du Premier ministre de la République Française. Il est constitué de 27 personnes d'horizons différents, issues du monde académique et politique, des entreprises ou de la société civile, pour aborder de manière globale les enjeux éthiques du numérique et donc de l'IA en particulier. Son rôle est à la fois d'élaborer des avis sur les saisines qui lui sont adressées et d'effectuer un travail de veille pour éclairer les prises de décision individuelles et collectives.

Les trois saisines initiales du gouvernement portent sur les agents conversationnels, le véhicule autonome, et le diagnostic médical à l'ère de l'intelligence artificielle. Mais la crise sanitaire de la Covid-19 a entraîné une réflexion, des communiqués et des avis sur les usages massifs du numérique dans un contexte de confinement et sur l'utilisation du numérique dans une stratégie de déconfinement.

Le CNPEN souhaite collaborer étroitement avec d'autres comités éthiques de pays européens pour contribuer à une approche européenne des enjeux éthiques du numérique. Il est donc particulièrement soucieux que l'approche proposée par Le Livre Blanc soit conforme à des valeurs partagées mais aussi à des conditions de vies partagées par le plus grand nombre.

La réponse du CNPEN à cette consultation porte sur les enjeux éthiques de l'IA comprise comme la partie des sciences et technologies du numérique intégrant tout particulièrement l'apprentissage machine (cf. la caractérisation proposée dans le livre blanc).

Section 1 – Un écosystème d'excellence

Afin de construire un écosystème d'excellence capable de soutenir le développement et de favoriser l'adoption de l'IA dans tous les secteurs économiques de l'UE, le Livre blanc propose une série d'actions.

Selon vous, quelle est l'importance des six actions proposées à la section 4 du Livre blanc sur l'IA (de 1 à 5: 1 n'est pas important du tout, 5 est très important)?

	1 - Pas important du tout	2 - Pas important	3 - Neutre	4 - Important	5 -Très important	Sans avis
Coopération avec les États membres	○	○	○	○	X	○
Cibler les efforts de la communauté de la recherche et de l'innovation	○	○	○	○	X	○
Compétences	○	○	○	○	X	○
Accorder une place de choix aux PME	○	○	○	○	X	○
Partenariat avec le secteur privé	○	○	○	○	X	○
Encourager le secteur public à adopter l'IA	○	○	○	○	X	○

A. ***Coopération avec les Etats Membres (5)*** : Le CNPEN comprend de nombreuses personnes appartenant à la communauté de la recherche et de l'innovation dans le domaine de l'IA en particulier. Elles proviennent principalement d'universités et d'institutions du secteur public mais sont souvent engagées dans des partenariats avec le secteur privé aux niveaux français, européen et international. De ce point de vue le CNPEN considère qu'il est très important de cibler les efforts de la communauté de la recherche et de l'innovation dans le cadre d'une coopération privilégiée entre États membres de l'UE.

B. ***Cibler les efforts (5)*** : Voir la réponse précédente.

C. ***Compétences (5)*** : La question du développement des compétences en IA est importante. Même si les États membres ont déjà des compétences académiques et des formations de qualité et reconnues internationalement il faut renforcer les compétences académiques et les centres interdisciplinaires pour mieux gérer les applications en IA

D. *Accorder une place de choix aux PME (5)* : Il est aussi crucial d'accorder une place de choix aux PME pour les aider à maîtriser et adopter les outils de l'IA dans leurs domaines d'activités tout en veillant à ce que l'accès au financement via Invest EU prenne en compte des critères d'usage de l'IA en conformité avec les enjeux éthiques et sociétaux dans le cadre de la transition écologique et solidaire pour l'UE.

E. *Partenariat avec le secteur privé (5)* : Concernant le partenariat avec le secteur privé, le CNPEN est attentif aux enjeux de souveraineté nationale et européenne (voir aussi le rapport[115] de la CERNA) et au risque d'érosion du patrimoine que constituent les données publiques si elles sont accessibles au secteur privé sans garanties suffisantes contre d'éventuels usages détournés. On pense en particulier aux données de santé, mais cela peut concerner d'autres corpus de données par exemple sur la mobilité des personnes et des biens, l'habitat et plus généralement toutes les ressources vitales. Il est donc indispensable d'assortir ces partenariats public-privé de règles de transparence, de contrôle et de réversibilité, voire de réciprocité d'accès à d'autres données.

F. *Encourager le secteur public à adopter l'IA (5)* : Enfin le CNPEN considère qu'il est effectivement souhaitable d'encourager le secteur public à adopter l'IA. Il existe plusieurs avantages à cette adoption : tout d'abord, l'acquisition de compétences en IA par l'administration, puis l'acculturation de nos concitoyens grâce à la multiplication des interactions avec l'IA. Enfin, l'adoption de la technologie par l'administration stimulera l'innovation et la commande publique en matière d'IA, qui dynamisera potentiellement le secteur des start-ups. Cependant, l'IA devra être un outil d'amélioration du service et non un remplacement des personnes qui le fournissent, et l'interaction humaine devrait rester la norme en particulier pour les usagers qui en auraient besoin dont les personnes isolées ou vulnérables ou ayant des difficultés d'accès aux interfaces numériques ou de maîtrise des outils numériques.

D'autres actions devraient-elles être envisagées?

Le CNPEN considère que l'Europe a un rôle particulier à jouer dans la coopération internationale externe à l'Union Européenne, en particulier avec les pays ACP (Afrique-Caraibes-Pacifique), pour le développement d'une IA de confiance et conforme aux valeurs éthiques partagées par les États membres et mentionnées dans le Livre Blanc (section 4 – H aspects internationaux). Pour mieux peser dans les négociations dans les grandes institutions internationales (ONU, G7, G20, OCDE, UNESCO, OMC, UIT etc.) il faudrait que les États membres de l'UE y parlent d'une même voix en se coordonnant au préalable.

[115] https://www.allistene.fr/files/2018/10/55708_AvisSouverainete-CERNA-2018.pdf

Une révision du plan coordonné dans le domaine de l'IA (action 1)

En tenant compte des résultats de la consultation publique sur le Livre blanc, la Commission proposera aux États membres une révision du plan coordonné en vue d'une adoption d'ici à la fin 2020

Selon vous, dans quelle mesure est-il important, dans chacun de ces domaines, d'aligner les politiques et de renforcer la coordination, comme décrit à la section 4.A du Livre blanc (de 1 à 5: 1 n'est pas important du tout, 5 est très important) ?

	1 - Pas important du tout	2 – Pas important	3 – Neutre	4 - Important	5 – Très important	Sans avis
Renforcer l'excellence dans la recherche	○	○	○	○	X	○
Établir des centres d'essai constituant une référence mondiale pour l'IA	○	○	○	○	X	○
Encourager le secteur public à adopter l'IA	○	○	○	○	X	○
Accroître le financement des start-ups innovantes dans le domaine de l'IA	○	○	○	○	X	○
Développer les compétences en matière d'IA et adapter les programmes de formation existants	○	○	○	○	X	○
Construire l'espace européen des données	○	○	○	○	X	○

En cohérence avec ses réponses aux questions précédentes, le CNPEN considère qu'il est très important de renforcer l'excellence dans la recherche, d'établir des centres d'essai constituant une référence mondiale pour l'IA, d'encourager le secteur public à adopter l'IA et d'accroître le financement des start-ups innovantes dans le domaine de l'IA,

De même le développement des compétences en matière d'IA et l'adaptation des programmes de formation IA sont jugés très important non seulement pour renforcer les compétences académiques, mais aussi pour favoriser l'adoption de l'IA à bon

escient par les entreprises, en particulier les PME, et par le secteur public, et surtout pour permettre l'acculturation des populations ayant des difficultés de maîtrise des outils numériques.

Quant à encourager le secteur public à adopter l'IA, le CNPEN émet la même réserve que précédemment, c'est-à-dire que cette adoption soit justifiée et maintienne une relation humaine entre l'administration et les citoyens, en particulier les personnes isolées ou vulnérables et ayant des difficultés d'accès aux interfaces numériques ou de maîtrise des outils numériques.

Enfin la construction d'un espace européen des données est très importante pour i) éviter la fragmentation des systèmes nationaux, ii) élaborer un standard européen pour le format des données, facteur d'interopérabilité et de rayonnement international, et iii) présenter un front commun plus fort dans la capacité de négociation de l'UE avec de grands acteurs privés extra-européens. Cet espace européen des données devra être soumis au contrôle démocratique du Parlement Européen, au contrôle des organes de supervision et aux avis consultatifs d'autres instances européennes telles que le Comité Economique et Social Européen (CESE).

D'autres domaines devraient-ils être envisagés ?

Le CNPEN souhaiterait que les pays membres de l'UE se dotent de comités consultatifs nationaux d'éthique du numérique et de l'IA et que ceux-ci se coordonnent au sein d'un comité consultatif européen.

Une communauté de la recherche et de l'innovation unie et renforcée qui vise l'excellence

Il sera essentiel d'unir les forces à tous les niveaux, de la recherche fondamentale jusqu'au déploiement, afin de surmonter la fragmentation et de créer des synergies entre les réseaux d'excellence existants.

Selon vous, quelle est l'importance des trois actions proposées dans les sections 4.B, 4.C et 4.E du Livre blanc sur l'IA (de 1 à 5: 1 n'est pas important du tout, 5 est très important)?

	1 - Pas important du tout	2 - Pas important	3 - Neutre	4 - Important	5 - Très important	Sans avis
Soutenir l'établissement d'un centre «phare» pour la recherche, qui soit de calibre mondial et capable d'attirer les cerveaux les plus brillants	○	○	X	○	○	○
Créer un réseau des centres d'excellence existants dans le domaine de la recherche en IA	○	○	○	○	X	○
Mettre en place un partenariat public-privé pour la recherche industrielle	○	○	○	○	X	○

A. ***Soutenir l'établissement d'un centre «phare» (3)*** : Le CNPEN est réservé sur la création d'un seul « centre phare » européen sur l'IA qui devrait coordonner les divers centres de compétence actuels. Plusieurs instituts de recherche européens en IA ont déjà une masse critique et pourraient constituer autant de « centres phares » interdisciplinaires européens de calibre mondial sur l'IA.

B. ***Créer un réseau des centres d'excellence (5)*** : En revanche il paraît très important, plus opérationnel et efficace de créer un réseau des centres d'excellence existants dans le domaine de la recherche en IA.

C. ***Mettre en place un partenariat public-privé (5)*** : La mise en place d'un partenariat public-privé pour la recherche industrielle est jugée importante pourvu que les relations établies avec les grands groupes privés internationaux soient suivies et auditées pour s'assurer que la recherche industrielle menée en Europe soit bien au service d'une souveraineté européenne.

D'autres actions visant à renforcer la communauté de la recherche et de l'innovation devraient-elles se voir accorder une priorité?

Le CNPEN encourage les programmes de recherche collaborative, multidisciplinaires et à long terme, et pas uniquement les projets individuels ou des projets ciblés à court terme.

Une attention particulière pour les petites et moyennes entreprise (PME)

La Commission collaborera avec les États membres pour faire en sorte qu'au moins un pôle d'innovation numérique par État membre ait un niveau élevé de spécialisation en IA.

Selon vous, quelle est l'importance de chacune de ces missions des pôles d'innovation numérique spécialisés mentionnés à la section 4.D du Livre blanc en ce qui concerne les PME (de 1 à 5: 1 n'est pas important du tout, 5 est très important)?

	1 - Pas important du tout	2 -Pas important	3 - Neutre	4 - Important	5 - Très important	Sans avis
Contribuer à sensibiliser les PME aux avantages potentiels de l'IA	○	○	○	X	○	○
Donner accès aux centres d'essai et de référence	○	○	○	X	○	○
Promouvoir le transfert de connaissances et soutenir le développement de l'expertise en matière d'IA pour les PME	○	○	○	○	X	○
Soutenir des partenariats entre les PME, les grandes entreprises et les universités autour de projets d'IA	○	○	○	○	X	○
Fournir des informations sur le financement en fonds propres pour les start-ups dans le domaine de l'IA	○	○	○	X	○	○

Le CNPEN souligne l'importance de sensibiliser les PME non seulement aux avantages potentiels de l'IA, mais aussi aux risques liés à l'IA, aux aspects éthiques et juridiques de la conception et de l'usage des outils numériques et des algorithmes d'IA et à leurs impacts sociétaux. L'IA n'est pas toujours la solution la plus appropriée. Ceci implique en particulier de développer et proposer des formations spécifiques.

Une expertise interne aux PME en matière d'IA étant difficile à entretenir et capitaliser le CNPEN considère que l'accès direct des PME aux centres d'essai et de référence leur permettrait d'une part d'expérimenter et d'autre part d'interagir avec les innovations élaborées par d'autres.

Les partenariats entre PME, grandes entreprises et universités autour de projets d'IA sont fondamentaux pour le transfert de connaissances et le développement d'expertises et de conseils en matière d'IA qui puissent être mis à disposition des PME.

Section 2 – Un écosystème de confiance

Le chapitre 5 du Livre blanc définit des options en vue d'un cadre réglementaire pour l'IA.

Selon vous, quelle est l'importance des préoccupations suivantes concernant l'IA (de 1 à 5 : 1 n'est pas important du tout, 5 est très important)

	1 - Pas important du tout	2 - Pas important	3 - Neutre	4 - Important	5 - Très important	Sans avis
L'IA peut compromettre la sécurité	○	○	○	○	X	○
L'IA peut porter atteinte aux droits fondamentaux (comme la dignité humaine, le respect de la vie privée, la protection des données, la liberté d' expression, les droits des travailleurs, etc.)	○	○	○	○	X	○
L'utilisation de l'IA peut entraîner des résultats discriminatoires	○	○	○	○	X	○

L'IA peut prendre des mesures dont les motifs ne peuvent pas être expliqués	○	○	○	○	X	○
Il peut être plus difficile pour les personnes ayant subi un préjudice du fait de l'utilisation de l'IA d'obtenir réparation	○	○	○	○	X	○
L'IA n'est pas toujours exacte	○	○	○	○	X	○

A. ***L'IA peut compromettre la sécurité (5) :*** La relation entre l'IA et la sécurité est ambivalente.

   D'un côté les technologies de l'IA peuvent présenter de nouveaux risques pour la sécurité. Au-delà des exemples bien connus (par ex. un accident lié au dysfonctionnement d'un véhicule autonome) on peut citer aussi le risque que l'IA puisse être utilisée par des pirates pour compromettre la sécurité en repérant, à partir de données, les habitudes des usagers, par exemple les mots de passe qu'ils ont l'habitude d'utiliser, etc. L'IA peut aussi être utilisée pour passer au crible des défenses informatiques et trouver des failles. Une IA digne de confiance nécessite des systèmes et algorithmes suffisamment sûrs, fiables et robustes pour répondre à des exigences de cybersécurité élevés en résistant aux attaques directes et aux tentatives plus subtiles de manipulation des données ou des algorithmes proprement dits. Ils doivent être fondés sur des mécanismes de « safety by design » et adopter les précautions nécessaires contre les risques de mésusages.
   De l'autre côté, et de façon plus positive, l'IA peut contribuer à renforcer la sécurité dans un certain nombre de domaines. À titre d'exemple des systèmes d'identité numérique, à condition qu'ils soient fiables et déployés sans biais liés au genre, au handicap, aux caractéristiques physiques ou l'origine ethnique, pourraient grandement améliorer la sécurité d'authentification, de connexion et de transactions. Par ailleurs, l'IA permet d'analyser tous les événements et de distinguer, parmi ceux-ci, les tentatives pour faire une brèche dans la sécurité des systèmes.

B. ***L'IA peut porter atteinte aux droits fondamentaux (5) :*** La mauvaise utilisation de l'IA pourrait porter atteinte à plusieurs droits fondamentaux. Le déploiement de certains systèmes de « reconnaissance émotionnelle », sans bases scientifiques solides et à des fins diverses, ou la mise en place de systèmes de surveillance sophistiqués fondés sur des techniques de reconnaissance faciale, illustrent certains risques pour les droits fondamentaux. Le scandale de Cambridge Analytica a par ailleurs montré qu'une mauvaise utilisation des données et de l'IA pourrait déstabiliser les socles démocratiques de nos sociétés européennes et servir à des opérations d'influence. Le CNPEN considère que l'Europe doit prêter

la plus grande attention à ces risques.

C. ***L'utilisation de l'IA peut entraîner des résultats discriminatoires (5) :*** Il s'agit ici d'une prolongation du point précédent. Les données utilisées par les systèmes d'IA peuvent être biaisées par des partis pris ou par des bases de données incomplètes ou reflétant des discriminations ou des biais humains. Les biais peuvent être présents à tous les stades de la conception et du déploiement (dont l'usage) des systèmes algorithmiques. De manière similaire, la manière dont les systèmes d'IA et les algorithmes sont construits peut également être entachée de biais ou aboutir à des inégalités de traitement, voire les systématiser ou les amplifier. Les systèmes de l'IA doivent être fondés sur le respect de la dignité humaine et de l'égalité de traitement, sans discrimination aucune, tout en prêtant une attention particulière à la sous-représentation de certaines catégories de population (femmes, certains groupes sociaux…) et à la situation des personnes vulnérables ainsi qu'aux questions d'accessibilité. En même temps, et de façon plus optimiste, le CNPEN considère que l'utilisation de l'IA peut aussi contribuer à éliminer les biais humains et à améliorer la situation des personnes handicapées, vulnérables ou à autonomie réduite.

D. ***L'IA peut prendre des mesures dont les motifs ne peuvent pas être expliqués (5) :*** L'explicabilité est essentielle, surtout quand l'utilisation de l'IA aboutit à des décisions affectant des personnes et leurs droits. Elle est indispensable, par exemple, pour justifier les décisions calculées dans les systèmes critiques, les systèmes d'affectation dans l'enseignement, l'aide au recrutement, la justice, etc. L'explicabilité contribuera à construire la confiance des citoyens à l'égard de ces technologies. Actuellement, un champ de recherche émerge afin d'améliorer l'explicabilité et la transparence des systèmes d'apprentissage ainsi que leur adaptation en contexte et l'adéquation de l'apprentissage à ce qu'en attend l'humain. Ainsi, il ne s'agit plus seulement de construire des modèles par apprentissage machine sans comprendre mais bien d'essayer de les expliquer. Voir l'avis de la CERNA, publiée en juin 2017, sur l'Ethique de la recherche en apprentissage machine[116].

E. ***Il peut être plus difficile pour les personnes ayant subi un préjudice du fait de l'utilisation de l'IA d'obtenir réparation (5) :*** Il s'agit d'une préoccupation importante qui appelle en effet un certain nombre de points d'attention s'agissant de la réparation non seulement du préjudice subi à titre *individuel* mais également de la réparation du préjudice *collectif.* Les règles existantes ne permettent pas nécessairement de signaler les discriminations subies par un groupe d'individus visé par un traitement algorithmique, au-delà de la somme des individus. Comme le soulignent certains rapports (voir par exemple le rapport de la CNIL[117] ou le rapport de la mission présidée par Cédric Villani[118]), plusieurs algorithmes fonctionnent en effet non à l'échelle de la personne mais à celle du groupe et les données ne sont pas tant granulaires que réticulaires, c'est-à-dire organisées en réseau. Ils peuvent dès lors être exploités afin de produire des corrélations concernant des segments ou groupes d'individus, potentiellement exposés à certains risques de discrimination. Cela appelle par conséquent une réflexion sur ces enjeux éthiques s'agissant de cette dimension

[116] http://cerna-ethics-allistene.org/digitalAssets/53/53991_cerna___thique_apprentissage.pdf
[117] https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_garder_la_main_web.pdf
[118] https://www.aiforhumanity.fr/pdfs/9782111457089_Rapport_Villani_accessible.pdf

collective et les solutions possibles.

F. *L'IA n'est pas toujours exacte (5) :* Les techniques d'apprentissage machines ne sont en général pas exactes au sens propre, mais peuvent fournir des approximations qui peuvent être intéressantes. Par ailleurs, il va de soi qu'un système qui est systématiquement faux ou approximatif est problématique. Il faudrait donc prévoir des méthodes et des critères de validation de l'apprentissage machine ainsi que des procédures de maintenance et s'intéresser aussi à la question importante de la reproductibilité des résultats.

Avez-vous d'autres préoccupations concernant l'IA qui ne sont pas mentionnées ci-dessus? Veuillez préciser:

D'autres enjeux éthiques importants sont soulignés dans l'avis de 2017 la CERNA sur l'Ethique de la recherche en apprentissage machine.

Trois problèmes de premier plan provoquent surtout des tensions éthiques : a) la spécification d'un système d'IA qui ne peut saisir complètement et correctement la définition d'un concept en langue naturelle, d'où l'inexactitude inhérente qui induit des erreurs d'interprétation ; b) l'instabilité de l'apprentissage d'un système d'IA qui ne classifiera pas « humainement » ou « correctement » une donnée qui ne faisait pas partie de son corpus d'apprentissage, provoquant de multiples problèmes de sécurité; c) la vérification d'un système d'IA dont on ne peut prouver que l'apprentissage respectera un cadre prédéfini en toutes circonstances, ce qui pose des question de responsabilité).

Plus largement, et en continuation de la discussion sur l'explicabilité, se pose la question des actions « inhumaines » de la part des systèmes d'IA, des interprétations données à ces actions par les utilisateurs et des changements de comportement des utilisateurs humains qui interagissent avec de tels systèmes.

Pensez-vous que les préoccupations exprimées ci-dessus peuvent être résolues par la législation européenne applicable? Dans la négative, estimez- vous qu'il devrait y avoir de nouvelles règles spécifiques pour les systèmes d'IA?

- La législation actuelle est amplement suffisante
- La législation actuelle peut présenter quelques lacunes
- Une nouvelle législation s'impose
- Autre Sans avis

Nous avons aujourd'hui un corpus de règles très important découlant d'instruments divers adoptés au fil du temps au sein de l'Union Européenne (sans parler d'autres règles et standards internationaux). Ces règles (telles que celles contenues, par exemple, dans le RGPD) sont « technologiquement neutres » (c'est à dire qu'elles ne sont pas spécifiques de technologies particulières) et restent pleinement applicables en matière d'IA. Elles constituent une bonne base de départ pour la régulation de l'IA et pour répondre aux risques susmentionnés.

Néanmoins, le CNPEN considère que le cadre législatif pourrait être amélioré et ceci pour plusieurs raisons.

- Premièrement, en l'état actuel il existe un risque de fragmentation du fait de divergences nationales dans l'application des règles existantes. Il serait donc utile d'assurer progressivement une interprétation uniforme des règles existantes par les organes de contrôle, les régulateurs, voire le législateur européen. À titre d'exemple, le Comité Européen de Protection des Données a un rôle important à jouer en ce qui concerne l'application du RGPD en matière d'IA.

- Deuxièmement, il est clair que, dans certains domaines, les règles existantes pourraient ne pas suffire et que l'on pourrait avoir besoin d'adapter le cadre législatif existant, voire d'adopter des nouvelles règles, pour faire face à un certain nombre de situations et de risques (voir, par exemple, nos commentaires sur la responsabilité dans la Section 3). Ceci pourrait être particulièrement utile pour mieux protéger les droits fondamentaux ou pour améliorer le régime juridique de responsabilité afin de garantir un système plus efficace et équitable d'indemnisation pour les dommages causés par l'utilisation d'IA.

- Enfin, le CNPEN considère qu'il est nécessaire de s'assurer que le cadre réglementaire existant tient suffisamment compte d'une série de principes éthiques nécessaires pour bâtir une IA de confiance.

Si vous pensez que de nouvelles règles sont nécessaires pour les systèmes d'IA, êtes-vous d'accord avec le fait que l'introduction d'exigences obligatoires nouvelles devrait être limitée aux applications à haut risque (dans lesquelles le préjudice éventuel causé par le système d'IA est particulièrement élevé)?

- Oui
- Non
- Sans Avis
- Autre (veuillez préciser):

Une approche réglementaire fondée sur une analyse de risques semble justifiée, tout comme la préoccupation de la Commission de ne pas s'engager dans une sur-réglementation européenne qui pourrait freiner l'innovation et le déploiement des effets bénéfiques multiples attendus par l'IA.

Il est important néanmoins d'évaluer les besoins en matière de régulation au cas par cas. Le critère pour l'adoption de règles pourrait ne pas être exclusivement le risque d'un préjudice « particulièrement élevé » mais aussi d'autres critères, y compris un risque important de violation des principes éthiques. Comme expliqué en introduction, les saisines initiales du CNPEN concernent trois domaines dont deux seulement (santé et véhicules connectés) semblent répondre à la définition de « haut risque » de la Commission. Les agents conversationnels présentent pourtant de « haut risques » dans certains domaines, par exemple lorsqu'ils sont utilisés avec reconnaissance faciale (et/ou audio) des émotions dans le cadre du recrutement avec des risques élevés de discrimination.

Ces situations mériteraient considération dans une approche réglementaire. Il serait peu satisfaisant, d'un point de vue éthique, que des dommages subis par des individus ne

soient pas indemnisés ou pris en considération car d'une part ils se situent dans la « zone grise » de l'arsenal réglementaire existant et, d'autre part, les institutions européennes n'auraient pas souhaité combler les lacunes existantes considérant qu'il ne s'agit pas là de domaines « à haut risque ».

Êtes-vous d'accord avec l'approche proposée à la section 5.B du Livre blanc afin de déterminer si une application de l'IA est «à haut risque» ?

- Oui
- Non
- Sans Avis
- Autre (veuillez préciser):
-

L'approche proposée constitue un bon point de départ mais devrait être affinée afin de mieux parvenir à une définition satisfaisante de la notion de « haut risque ». Comme la Commission elle-même le reconnaît, il peut exister des situations (des cas exceptionnels ?) dans lesquelles, « compte tenu des risques, l'utilisation d'applications d'IA à certaines fins devrait être considérée comme étant à haut risque en soi, c'est-à-dire indépendamment du secteur concerné ». Il en résulte une double incertitude : quant aux situations précises où le secteur n'est plus un critère déterminant ; et quant à la personne qui va procéder à cette évaluation et aux méthodes utilisées. On pourrait craindre que, compte tenu de ces incertitudes, les développeurs et opérateurs de systèmes IA puissent revendiquer ce pouvoir d'appréciation. Le fait de décider si un système d'IA (et les technologies connexes) doit être considéré comme étant « à haut risque » devrait toujours découler d'une évaluation impartiale, réglementée et externe prenant en compte non seulement l'application elle-même, mais aussi son intégration dans un système d'information plus global. L'évaluation du risque doit être fondée non seulement sur la gravité du dommage potentiel mais aussi sur la gravité de la violation des principes éthiques sous-jacents.

Si vous le souhaitez, veuillez indiquer quelle est, de votre point de vue, l'application ou l'utilisation de l'IA la plus préoccupante («à haut risque»):

Si les systèmes d'armes létaux autonomes viennent immédiatement à l'esprit, d'autres applications pourraient aussi susciter des préoccupations éthiques tout aussi fondamentales. À titre d'exemple les applications suivantes pourraient être très préoccupantes : les systèmes de « notation sociale » des citoyens d'un pays fondés sur une évaluation de leur comportement et de leur « intégrité éthique » ; les systèmes de surveillance de masse fondés sur la reconnaissance biométrique ; ou encore certains systèmes décisionnels fondés sur les réactions émotionnelles comme par exemple la reconnaissance d'émotions faciales ou audio pour le recrutement, la détection du mensonge aux frontières, la détection de l'attention des élèves à l'école, etc.

Selon vous, quelle est l'importance des exigences obligatoires suivantes énoncées dans un éventuel futur cadre réglementaire pour l'IA (section 5.D du Livre blanc) (de 1 à 5: 1 n'est pas important du tout, 5 est très important)?

	1 — Pas important du tout	2 - Pas important	3 - Neutre	4 - Important	5 - Très important	Sans avis
Qualité des ensembles de données d'entraînement	○	○	○	○	X	○
Conservation des dossiers et des données	○	○	○	X	○	○
Informations sur la finalité et la nature des systèmes d'IA	○	○	○	○	X	○
Robustesse et précision des systèmes d'IA	○	○	○	○	X	○
Contrôle humain	○	○	○	○	X	○
Règles claires en matière de sécurité et de responsabilité	○	○	○	○	X	○

A. *Qualité des ensembles de données d'entraînement (5)* : La qualité et l'intégrité des données sont essentielles au bon fonctionnement des systèmes IA.

B. *Conservation des dossiers et des données (4)* : Il convient ici de distinguer deux situations. D'une part, il est très important d'établir des exigences relatives à la conservation des dossiers de programmation de l'algorithme et des données utilisées pour entraîner les systèmes d'IA. La traçabilité des systèmes d'IA doit en effet être assurée. Il est donc important de pouvoir tracer l'ensemble du processus qui a abouti à la prise d'une décision et d'enregistrer l'ensemble des décisions prises par les systèmes.
En revanche, la conservation des données elles-mêmes pourrait s'avérer problématique à trois titres :

- Premièrement la conservation de grandes masses de données pourrait augmenter les risques d'atteinte à la vie privée et d'exploitation malveillante.
- Deuxièmement la conservation systématique de grandes masses de données a un impact énergétique et environnemental non négligeable. Le CNPEN considère que l'IA doit être développée et utilisée de manière à garantir un respect optimal de l'environnement et à réduire autant que possible son empreinte écologique, afin de soutenir la réalisation des objectifs fixés en matière de neutralité climatique et d'économie circulaire.

- Troisièmement la conservation des données personnelles doit être conforme aux règles en matière de protection des données et de la vie privée qui imposent souvent aux acteurs privés et publics des délais de rétention courts et/ou des limitations dans le temps liées à la durée du consentement et au principe de minimisation des données.

C. *Informations sur la finalité et la nature des systèmes d'IA (5)* : L'information sur la finalité d'un système d'IA (les objectifs poursuivis), ses capacités et ses limites et les conditions dans lesquelles il devrait fonctionner sont importantes non seulement pour les opérateurs et les utilisateurs mais aussi, éventuellement, pour les autorités compétentes. Il est important, de façon générale, de respecter le principe de transparence et d'information. Par ailleurs la Commission souligne avec raison que des informations devraient être clairement fournies aux citoyens lorsqu'ils interagissent avec un système d'IA et non avec un être humain.

D. *Robustesse et précision des systèmes d'IA (5)* : Comme déjà mentionné, la robustesse et la fiabilité des systèmes IA ainsi que leur cybersécurité sont des conditions essentielles pour parvenir à une IA de confiance. Les systèmes d'IA devraient être fiables et intégrer des mécanismes de sécurité par conception (« safety by design ») et de sûreté. Voir aussi *supra* nos développements sur « l'exactitude » et le rapport qui y est mentionné.

E. *Contrôle humain (5)* : Le Livre Blanc intègre, à juste raison, la notion d'une Garantie Humaine de l'intelligence artificielle (*Human Oversight* ou *Human Warranty*). Ce principe a d'ores et déjà fait l'objet de travaux abondants dans le cadre du processus en cours de révision de la loi de bioéthique française sous l'égide du CCNE et des démarches initiées par le CNPEN.
Cette idée d'une Garantie Humaine de l'IA est issue d'un mouvement de propositions académiques, citoyennes mais aussi de professionnels de santé. Ce principe a été reconnu dans les avis 129 et 130 du CCNE et dans l'article 11 du projet de loi bioéthique en cours d'examen devant le Parlement français. Cette notion a également été portée dans le cadre des travaux en cours de la task-force sur la régulation de l'IA dans le cadre de l'Organisation Mondiale de la Santé.
Le concept de « Garantie Humaine » peut paraître abstrait mais il est, en réalité, très opérationnel. Dans le cas de l'IA, l'idée est d'appliquer les principes de régulation de l'intelligence artificielle en amont et en aval de l'algorithme lui-même en établissant des points de supervision humaine. Non pas à chaque étape, sinon l'innovation serait bloquée. Mais sur des points critiques identifiés dans un dialogue partagé entre les professionnels, les patients et les concepteurs d'innovation.
Dans le domaine de la santé, le CCNE a proposé que cette supervision puisse s'exercer avec le déploiement de **« collèges de garantie humaine »** associant médecins, professionnels paramédicaux et représentants des usagers. Leur vocation serait d'assurer *a posteriori* une révision de dossiers médicaux pour porter un regard humain sur les options thérapeutiques conseillées ou prises par l'algorithme. L'objectif consiste à s'assurer « au fil de l'eau » que l'algorithme reste sur un développement de *Machine Learning* à la fois efficace médicalement et responsable éthiquement. Les dossiers à auditer pourraient être définis à partir d'événements indésirables constatés, de critères prédéterminés ou d'une sélection aléatoire. Un premier cas pilote de collège de garantie humaine est en phase de déploiement sous l'égide de l'Union française pour la santé bucco-dentaire

(UFSBD) : il mettra en œuvre, dans le cadre d'un programme de financements innovants de la Sécurité sociale, une supervision pour un programme d'IA applicable aux soins dentaires pour 48 EHPAD et mis en œuvre par la start-up française *Dental Monitoring*. Cette méthodologie est, en outre, mobilisée dans le cadre des travaux de DRIM France IA, démarche de rassemblement des acteurs de la radiologie française pour le développement responsable de l'IA dans cette discipline.
Cette méthode de supervision humaine au fil de l'eau associant innovateurs en IA, experts techniques et représentants des bénéficiaires finaux est transposable dans d'autres domaines économiques et sociaux que la santé.

F. ***Règles claires en matière de sécurité et de responsabilité (5)*** : Nous n'avons aucun doute sur le fait que l'existence de règles claires en matière de sécurité et de responsabilité est indispensable pour assurer la nécessaire sécurité et visibilité juridiques et garantir la protection des consommateurs, la sécurité juridique pour les entreprises et un rôle et des limites clairs pour les régulateurs et les pouvoirs publics.

En plus de la législation existante de l'UE, en particulier le cadre relatif à la protection des données, et notamment le règlement général sur la protection des données et la directive en matière de protection des données dans le domaine répressif, ou, le cas échéant, les nouvelles exigences obligatoires éventuellement prévues plus haut (voir la question ci-dessus), estimez-vous que l'utilisation de systèmes d'identification biométrique à distance (par exemple, la reconnaissance faciale) et d'autres technologies susceptibles d' être utilisées dans les espaces publics doit faire l'objet d'orientations ou de réglementations supplémentaires au niveau de l'UE?

- Aucune orientation ou réglementation supplémentaire ne s'impose
- Les systèmes d'identification biométrique ne devraient être autorisés dans les espaces accessibles au public que dans certains cas ou si certaines conditions sont remplies (veuillez préciser)
- Il faudrait imposer d'autres exigences particulières, en plus de celles mentionnées dans la question ci-dessus (veuillez préciser)
- L'utilisation de systèmes d'identification biométrique dans les espaces accessibles au public, à titre d'exception à l'interdiction générale actuelle, ne devrait être possible qu'après la mise en place d'une orientation ou d'une législation spécifique au niveau de l'UE
- Les systèmes d'identification biométrique ne devraient jamais être autorisés dans les espaces accessibles au public
- Sans avis

Veuillez préciser votre réponse:

Il est très satisfaisant qu'en Europe, contrairement à d'autres parties du monde, nous disposions déjà de règles importantes en matière de cadrage de la reconnaissance faciale. Des instruments comme la Charte des droits fondamentaux de l'UE, la Convention européenne des droits de l'homme, le RGPD ou la directive police-justice posent déjà un

cadre réglementaire important pour l'utilisation de techniques de reconnaissance faciale (TRF) par le secteur privé ou le secteur public.

Nous considérons, néanmoins, que, compte tenu des risques particulièrement importants existant dans ce domaine, les règles devraient être précisées et complétées. Premièrement, il y a un risque important d'interprétation divergente des règles existantes par les autorités de régulation et de contrôle dans les pays européens. Deuxièmement, la transparence en Europe sur les projets d'utilisation des TRF par le privé et le public devrait être assurée. Troisièmement, plutôt que d'entrer de façon aveugle dans une « course » aux TRF avec les États-Unis ou la Chine, l'Europe devrait donner l'exemple en se focalisant sur les problèmes que la reconnaissance faciale pourrait résoudre et en insistant sur les principes de nécessité et de proportionnalité. Quatrièmement, une réglementation claire et homogène au sein de l'EU favoriserait la dynamique de l'innovation et l'acceptabilité des citoyens, en prévenant d'éventuelles dérives. Des interventions législatives ou réglementaires pourraient s'avérer nécessaires pour fixer les « lignes rouges », aider à établir des lignes directrices là où l'utilisation des TRF se justifie et prévoir des garanties, contrôles et voies de recours appropriés. De façon plus générale, les TRF dans l'espace public posent des dilemmes éthiques particulièrement importants qui devraient d'abord être analysés au niveau politique après un débat démocratique. Le CNPEN espère pouvoir contribuer dans l'avenir à ce débat tant sur le plan national que sur le plan européen.

Estimez-vous qu'un système de label non obligatoire (section 5.G du Livre blanc) serait utile pour les systèmes d'IA qui ne sont pas considérés comme étant à haut risque, en plus de la législation existante?

- Extrêmement utile
- Très utile
- Plutôt inutile
- Tout à fait inutile
- Sans avis

Avez-vous d'autres suggestions sur un système de label non obligatoire?

Un système de label non obligatoire peut être utile pour des systèmes d'IA qui ne sont pas considérés à haut risque. Mais il faut veiller à ce que ces labels ne soient pas l'apanage de groupes industriels qui s'auto-labelliseront. En complément, cela nécessite donc la mise en place d'organismes de certification et d'éducation de la population et l'on préconise plutôt le respect de normes et de standards internationaux précis et auditables.

1.1.1

Quel est le moyen de garantir une IA digne de confiance, sûre et respectueuse des règles et valeurs européennes?

- Évaluation préalable de la conformité des applications à haut risque avec les exigences identifiées (avant de mettre le système sur le marché)
- Évaluation a posteriori de la conformité des applications à haut risque au moyen d'une procédure d'évaluation externe de la conformité

- Surveillance a posteriori du marché après la mise sur le marché du produit ou du service à haut risque reposant sur l'IA et, le cas échéant, contrôle du respect assuré par les autorités compétentes concernées
- **Combinaison de mécanismes d'évaluation préalable de la conformité et de contrôle a posteriori du respect**
- Autre système de contrôle du respect
- Sans avis

Veuillez préciser tout autre système de contrôle du respect

Tout système d'IA considéré « à haut risque » devra être soumis une homologation et une certification de conformité a priori. De plus, dans la mesure où la réponse d'un algorithme d'IA est susceptible d'évoluer quand il s'agit d'un apprentissage supervisé ou non supervisé ou par renforcement, en particulier si l'apprentissage est réalisé en continu et si le domaine d'application est ouvert, il est indispensable de soumettre le système à des tests réguliers et normés pour vérifier que la réponse ne s'écarte pas du cadre de l'homologation. Cela peut passer a minima par des contrôles techniques réguliers, comme ceux déjà pratiqués pour les automobiles, mais aussi nécessiter des étapes de re-homologation et re-certification des logiciels d'IA.

Section 3 – Implications de l'intelligence artificielle, de l'internet des objets et de la robotique en matière de sécurité et de responsabilité

L'objectif général des cadres juridiques en matière de sécurité et de responsabilité est de garantir que tous les produits et services, y compris ceux qui intègrent des technologies numériques émergentes, fonctionnent de manière sûre, fiable et cohérente et que les dommages qui se sont produits soient réparés efficacement.

La législation actuelle sur la sécurité des produits offre déjà une interprétation étendue de la notion de sécurité qui permet de protéger contre tous types de risques liés aux produits en fonction de leur utilisation. Toutefois, quels risques particuliers découlant de l'utilisation de l'IA conviendrait-il, selon vous, de préciser davantage afin d'assurer une plus grande sécurité juridique?

- Les risques liés à la cybersécurité
- Les risques pour la sécurité des personnes
- Les risques liés à la perte de connectivité
- Les risques pour la santé mentale

Les risques liés à la cybersécurité sont de loin les plus importants car les cyberattaques peuvent avoir des conséquences multiples et néfastes. Il est néanmoins rassurant que toutes les parties prenantes ont conscience de ces risques ce qui devrait permettre une prise en compte adéquate de ce risque dans le cadre de futures évolutions normatives. D'autres risques, néanmoins, tels que ceux relatifs à la santé mentale décrits dans le Livre Blanc, sont très peu pris en considération par les règles existantes. Il serait dès lors utile que les risques pour la santé mentale soient explicitement couverts par le concept de sécurité des produits dans le cadre législatif.

Selon vous, faut-il élargir à d'autres risques afin d'assurer une plus grande sécurité juridique ?

N/A

Pensez-vous que le cadre législatif relatif à la sécurité devrait envisager de nouvelles procédures d'évaluation des risques pour les produits faisant l'objet de changements importants au cours de leur durée de vie?

- Oui
- Non
- Sans avis

Le développement des outils numériques et des algorithmes d'IA permettant de rejouer des séquences préalablement enregistrées, ainsi que la simulation numérique de mises en scène réalistes de cas d'usage comportant des risques offrent de grandes possibilités de faire évoluer les procédures d'évaluation des risques pour les produits faisant l'objet de changements importants au cours de leur durée de vie. Cela offre de nouvelles possibilités de virtualisation des tests d'homologation et de certification par des « jumeaux numériques ». De plus, en développant des scénarios (*serious games)* les outils de

simulation peuvent constituer des outils d'aide à la décision pour des comités d'évaluation impliquant des représentants des diverses parties prenantes d'un domaine d'application et d'un écosystème spécifique (mobilité, énergie, santé, défense etc.).

Avez-vous d'autres considérations concernant les procédures d'évaluation des risques?

N/A

Pensez-vous que le cadre législatif actuel de l'UE en matière de responsabilité (directive sur la responsabilité du fait des produits) devrait être modifié afin de mieux couvrir les risques engendrés par certaines applications de l'IA?

- Oui
- Non
- Sans avis

Avez-vous d'autres considérations concernant la question ci-dessus?

Comme en matière de régulation en général (*supra*), le CNPEN n'est pas favorable à une refonte complète des régimes de responsabilité existants – et de la directive sur la responsabilité du fait des produits (directive 85/374/CEE) – qui fonctionnent plutôt bien. Il considère que la mise en place de règles de responsabilité très lourdes pourrait freiner l'innovation et s'avérer préjudiciable pour le développement de l'IA en Europe.

Le CNPEN note, néanmoins, que la directive sur la responsabilité du fait des produits a été adoptée en 1985, une époque antérieure à la prise en considération des risques associés à l'émergence des nouvelles technologies numériques et, surtout, de l'IA. Certes, les règles de la directive ne sont pas spécifiques à des technologies particulières et s'appliquent dont quelle que soit la technologie utilisée. Mais elles ne sont pas toujours en mesure de saisir les difficultés qui résultent de la complexité, la connectivité, l'opacité, la vulnérabilité et l'autonomie des systèmes d'IA. dé Le CNPEN considère donc que des ajustements spécifiques du cadre législatif actuel pourraient être nécessaires pour éviter que des personnes victimes de préjudices ou dont les biens sont endommagés se trouvent sans réparation. L'attention du législateur pourrait être portée sur des sujets tels que les suivants :

- Le fait que la directive repose sur le concept de « produit » (et de ses défauts), perçu essentiellement comme un objet alors que dans les systèmes d'IA les « produits » et les « services » interagissent de façon permanente (comme en témoigne l'exemple de la voiture connectée) ;
- Le fait que le concept de « défaut » d'un produit mériterait d'être précisé dans le cadre des caractéristiques très spécifiques des systèmes d'IA, voire des logiciels en général.

Pensez-vous que les règles nationales actuelles en matière de responsabilité devraient être adaptées en tenant compte du fonctionnement de l'IA afin de mieux garantir une réparation adéquate des dommages et une répartition équitable des responsabilités?

- Oui, pour toutes les applications de l'IA
- Oui, pour des applications de l'IA spécifiques
- Non
- Sans avis

Veuillez préciser les applications de l'IA:

Les droits nationaux en matière de responsabilité souffrent de fragmentation et ne comportent souvent pas de règles spécifiques en matière de responsabilité pour dommages causés par des systèmes d'IA. Sans énumérer ici les applications de l'IA spécifiques, il nous semble qu'il est nécessaire de procéder à une étude approfondie et secteur par secteur afin de tenir compte des éléments suivants :

- Les difficultés liées à la définition du dommage et des types de dommages indemnisés par les droits nationaux.
- Les difficultés liées à la nécessité pour la victime d'apporter la preuve de l'existence d'un lien de causalité qui pourrait s'avérer une véritable probatio diabolica quand le dommage résulte du dysfonctionnement d'un système d'IA. Apporter la preuve d'une discrimination résultant d'un traitement algorithmique constitue, par exemple, une difficulté essentielle au regard de l'opacité du système informatique.
- Ces difficultés probatoires ne se limitent pas d'ailleurs à l'établissement du seul lien de causalité. Elles portent également sur l'existence de la discrimination per se. En effet, comment le demandeur peut-il être à même d'établir l'effet discriminatoire d'une pratique, notamment lorsque les critères fondant la décision prise à l'issue d'un traitement algorithmique ainsi que leur pondération ne sont pas connus ? A défaut d'information sur ces critères, seule une analyse statistique des résultats produits par l'algorithme permettrait d'établir de tels faits. Mais une telle analyse ne saurait certainement être menée par le demandeur seul, s'il s'agit d'un individu contestant une décision prise à son encontre. Il convient alors de mener une réflexion sur le point de savoir comment remédier à de telles difficultés.
- La nécessité de repenser, en fonction de la situation, la répartition de la responsabilité entre le producteur, le fabricant, le développeur, l'opérateur, et l'utilisateur.
- La possibilité de prévoir différentes règles de responsabilité pour différents risques et, surtout, un système de facilitation de la preuve ou un régime de responsabilité stricte pour des systèmes d'IA « à haut risque ».
- La nécessité de définir si les systèmes d'IA identifiés comme « à haut risque » à des fins de responsabilité stricte devraient être les mêmes (ou plutôt plus restreints) que les systèmes « à haut risque » à des fins de régulation discutés dans la Section II de ce questionnaire et sur la base de quels critères distinguer les deux catégories.
- L'utilité ou non d'envisager un devoir de diligence accrue des développeurs, opérateurs et autres parties prenantes d'un système d'IA leur imposant de

sélectionner, d'exploiter, de surveiller et d'entretenir correctement la technologie utilisée.

- Le principe d'équivalence fonctionnelle qui devrait garantir que les personnes qui ont subi un dommage du fait de l'utilisation d'un système d'IA ne devraient pas être moins indemnisées que si le dommage provenait d'un système analogue déjà couvert par le droit européen ou les droits nationaux.

Avez-vous d'autres considérations concernant la question ci-dessus?

Le CNPEN souhaite rappeler la polémique suscitée début 2017 quand le Parlement Européen a proposé à la Commission Européenne, « la création d'une personnalité juridique spécifique aux robots » qui impliquerait que les robots pourraient être tenus pour civilement responsables des dommages qu'ils causeraient, ce qui obligerait leurs fabricants ou propriétaires à contracter des polices d'assurance couvrant les dommages potentiels causés par leurs robots.

Le Comité Economique et Social Européen (CESE) s'est opposé formellement à cette proposition pour deux raisons principales : i) « le risque moral inacceptable » que le fabricant n'assume plus sa responsabilité, transférée au robot (ou au système d'IA), au détriment d'une éthique de conception, et ii) « le risque d'utilisation impropre et d'abus d'une telle forme juridique » si les incidents consécutifs à une mauvaise utilisation peuvent être imputés à l'IA ou au robot intelligent par son propriétaire.

Le CNPEN considère que ce débat juridique et éthique est de première importance.

Merci pour votre contribution à ce questionnaire.

APPEL À CONTRIBUTIONS

LES ENJEUX ÉTHIQUES DES AGENTS CONVERSATIONNELS

Du 26 juin au 31 octobre 2020

https://www.ccne-ethique.fr/fr/actualites/cnpen-les-enjeux-ethiques-des-agents-conversationnels

COMMUNIQUÉ DE PRESSE

Le Comité national pilote d'éthique du numérique (CNPEN) a été créé en décembre 2019 à la demande du Premier ministre. Constitué de 27 membres, ce comité réunit des spécialistes du numérique, des philosophes, des médecins, des juristes et des membres de la société civile. L'une des trois saisines soumises par le Premier ministre au CNPEN concerne les enjeux éthiques des agents conversationnels, appelés communément *chatbots*, qui communiquent avec l'utilisateur humain par la voix ou par écrit. Ce travail du CNPEN vient en prolongation des travaux initiés par la CERNA, Commission d'éthique de la recherche en sciences et technologies du numérique de l'alliance Allistene.

Le présent appel vise à permettre une expression des parties prenantes et du public sur les enjeux éthiques liés aux *chatbots*. Nous sollicitons l'avis du lecteur en posant des questions. Chaque contributeur est invité à répondre soit à quelques questions de son choix soit à l'ensemble des questions posées. Les propos des contributeurs ne seront pas cités nommément dans le futur avis.

Envoi des réponses à l'adresse cnpen-consultation-chatbots@ccne.fr

Télécharger le document

LES ENJEUX ÉTHIQUES DES AGENTS CONVERSATIONNELS

Le Comité national pilote d'éthique du numérique (CNPEN) a été créé en décembre 2019 à la demande du Premier ministre. Constitué de 27 membres, ce comité réunit des spécialistes du numérique, des philosophes, des médecins, des juristes et des membres de la société civile. L'une des trois saisines soumises par le Premier ministre au CNPEN concerne les enjeux éthiques des agents conversationnels, appelés communément *chatbots*, qui communiquent avec l'utilisateur humain par la voix ou par écrit. Ce travail du CNPEN vient en prolongation des travaux initiés par la CERNA, Commission d'éthique de la recherche en sciences et technologies du numérique de l'alliance Allistene.

Dans ce document, nous sollicitons l'avis des lecteurs en posant des questions sur les enjeux éthiques liés aux chatbots. Chacun est invité à répondre soit à quelques questions de son choix soit à l'ensemble des questions posées.

Répondez-vous à ce questionnaire :

- *À titre personnel (préciser vos nom et prénom si vous le souhaitez)*
- *Au titre de vos activités professionnelles ou au nom d'une organisation :*
    - *Chercheur ou Institut de recherche (préciser le nom de votre institution)*
    - *Société ou groupe de sociétés (préciser laquelle)*
    - *Association de consommateurs ou assimilé (préciser laquelle)*
    - *Autorité publique (préciser laquelle)*
    - *Consultant professionnel*
    - *Think thank (préciser lequel)*
    - *Autre :*

Objectifs de ce document :

Le Comité national pilote d'éthique du numérique (CNPEN), créé en décembre 2019 sous l'égide du CCNE pour les sciences de la vie et de la santé, a été saisi par le Premier ministre pour élaborer en particulier un avis sur les enjeux éthiques des agents conversationnels (*chatbots*). Il a aussi dans ses objectifs « d'engager une discussion collective pour développer une approche partagée des innovations présentes et futures. Cette dimension est fondamentale pour s'assurer que la technique et l'innovation continuent à servir le bien commun. ». C'est pourquoi le Comité engage une consultation des parties prenantes et des citoyens avec pour objectifs de les sensibiliser aux enjeux éthiques et d'enrichir sa réflexion.

Utilisation et protection de vos données personelles :

Les données personnelles demandées (*adresse mail, nom, prénom, profession, institution de rattachement*) ou celles que vous pourriez fournir spontanément dans votre réponse au questionnaire ne seront traitées que si elles sont utiles à l'analyse et à la réflexion du comité. Toutes les données personnelles récoltées seront conservées sur les serveurs du CCNE ou de ses prestataires. Elles seront traitées de manière confidentielle uniquement par le personnel du CNPEN ou les membres du groupe de travail du CNPEN sur les agents conversationnels ; elles ne seront pas traitées de manière automatisées. Elles seront conservées au maximum dix-huit mois après la clôture de la consultation et jusqu'à douze mois après la publication de l'avis du comité.

Les résultats de cette analyse nourriront l'avis du comité sur les agents conversationnels, qui sera rendu public. Les contributions n'y seront pas citées nommément sans l'accord explicite de leurs auteurs.

Dans les conditions définies par la Loi Informatique et Libertés du 6 janvier 1978 et par le Règlement Européen sur la Protection des Données Personnelles entré en vigueur le 25 mai 2018, chaque contributeur bénéficie d'un droit d'accès aux données le concernant, de rectification, d'interrogation, de limitation, de portabilité et d'effacement. Chaque contributeur peut également, pour des motifs légitimes, s'opposer au traitement de ses données personnelles. Le contributeur peut exercer l'ensemble des droits mentionnés ci-dessus en s'adressant au CNPEN à l'adresse : cnpen-consultation-chatbots@ccne.fr.

INTRODUCTION

Qu'est-ce qu'un agent conversationnel ?

Un agent conversationnel, appelé communément chatbot, est un programme informatique qui interagit avec son utilisateur dans la langue naturelle de celui-ci. Ces termes regroupent tant les agents vocaux que les chatbots écrits.

Le plus souvent, un agent conversationnel ne constitue pas une entité indépendante mais il est intégré au sein d'un système ou d'une plate-forme numérique, comme un smartphone ou une enceinte vocale[119]. Sur le plan de l'apparence visuelle, les chatbots peuvent aussi être intégrés à un agent conversationnel animé, représenté en deux ou trois dimensions sur un écran, voire faire partie d'un robot social, y compris humanoïde. Le dialogue avec l'utilisateur ne représente alors qu'une des fonctions du système global.

L'histoire des agents conversationnels prend ses origines dans le jeu de l'imitation d'Alan Turing[120]. La compréhension du langage intéresse Turing dans la mesure où elle se manifeste à travers des réponses qui paraissent intelligibles et sensées à un examinateur (« test de Turing »). Dès 1991, un concours annuel est organisé afin de soutenir le développement de chatbots capables de passer le test de Turing.

Le premier agent conversationnel de l'histoire de l'informatique est le programme ELIZA de Joseph Weizenbaum[121], qui est aussi l'un des premiers leurres conversationnels. ELIZA simule un dialogue écrit avec un psychothérapeute rogérien en reformulant tout simplement la plupart des répliques de l'utilisateur « patient » sous forme de questions. Aujourd'hui, l'expression « effet ELIZA » désigne la tendance à assimiler de manière inconsciente le dialogue avec un ordinateur à celui avec un être humain.

D'un point de vue technique, comment ça marche ?

La conception et le fonctionnement d'un agent conversationnel se divisent en plusieurs modules de traitement automatique du langage naturel (TALN) : schématiquement, un chatbot peut inclure des modules de reconnaissance de la parole (pour les agents conversationnels vocaux), de traitement sémantique (hors et en contexte), de gestion de l'historique du dialogue, de gestion des stratégies de dialogue, d'accès aux ontologies, de gestion des accès aux connaissances externes (base de données ou internet), de génération de langage et de synthèse de la parole (pour les agents conversationnels vocaux).

Un agent conversationnel suit des règles décidées et transposées en code par des concepteurs humains ou obtenues par apprentissage. Les chatbots apprenants, par exemple XiaoIce de Microsoft Chine[122], sont aujourd'hui encore assez rares parmi les

---

119 "Google Assistant", "Google Home", "Apple Siri", "Amazon Alexa" et "Amazon Echo", "Yandex Alisa", "Mail.ru Marusia", "Baidu DuerOS", "Xiaomi XiaoAI", "Tencent Xiaowei", "Samsung Bixbi", "Orange Djingo", etc.

120 A. Turing, "Computing Machinery and Intelligence", *Mind* 59(236) 433–460, 1950.

121 J. Weizenbaum, "ELIZA - A Computer Program for the Study of Natural Language Communication between Man and Machine", *Communications of the Association for Computing Machinery* 9, 36-45, 1966.

122 Li Zhou, Jianfeng Gao, Di Li, and Heung-Yeung Shum, "The Design and Implementation of XiaoIce, an Empathetic Social Chatbot", *Computational Linguistics* 46(1), 53-93, 2020.

applications commercialisées, mais leur proportion n'aura de cesse de croître avec l'avancement de la maîtrise de cette technologie.

Ces dernières années, développer soi-même un chatbot rudimentaire ou dédié à une seule tâche est devenu relativement facile grâce à la disponibilité de nombreux outils de conception, comme "LiveEngage", "Chatbot builder", "Passage.ai", "Plato Research Dialogue System", etc.

Quelques défis de recherche concernant la conception des agents conversationnels

- Apprendre de manière adaptative en faisant évoluer la base de connaissances en cours d'utilisation.
- Être capable de converser librement sur des sujets génériques.
- Saisir le « sens commun », le caractère ironique ou le sens au « second degré » d'un énoncé
- Mettre en place une stratégie de dialogue.
- Détecter les émotions et les intentions de l'utilisateur.

Quelques défis de recherche concernant la compréhension des capacités des agents conversationnels par les utilisateurs

- Quelles données les chatbots enregistrent-t-ils ? Sont-elles anonymisées ?
- Comment peut-on mener des audits du comportement des chatbots (mesure automatique ou/et évaluation humaine) ?
- Les répliques sélectionnées par les chatbots sont-elles explicables ? Les chatbots peuvent-ils les rendre eux-mêmes plus compréhensibles ?
- Quels paramètres du profil de son interlocuteur les chatbots calculent-ils ? Les humains en sont-ils conscients ?
- L'idée que l'utilisateur se fait de la stratégie du chatbot correspond-elle à la stratégie réelle mise en place dans le chatbot ?

Questions éthiques

Le langage est un élément constitutif de l'identité de l'être humain et le fondement de sa vie en société. Les agents conversationnels sont ainsi naturellement comparés à un être humain, que leur interlocuteur soit informé, ou non, de leur caractère artificiel. Cet aspect naturel du dialogue est susceptible d'influer sur l'être humain : c'est le problème fondamental de l'éthique des chatbots. Leur déploiement étant un phénomène récent, on ne dispose pas de données expérimentales suffisantes pour évaluer leurs effets sur l'être humain à long terme.

Depuis peu, les performances de la reconnaissance de la parole permettent l'utilisation des interfaces vocales. Outre le dialogue langagier, la voix porte des informations de diverses natures, par exemple sur l'âge, le sexe, la corpulence, la langue maternelle, l'accent, les lieux de vie, le milieu socio-culturel, l'éducation, l'état de santé, la compréhension ou les émotions de la personne qui parle. De nombreuses questions éthiques sont liées à ces aspects de la vie humaine.

À l'instar des systèmes techniques en général et des systèmes autonomes en particulier (par exemple, la reconnaissance automatique d'images ou la conduite autonome des véhicules), les agents conversationnels doivent répondre à un grand nombre d'exigences en termes de sécurité, transparence, traçabilité, utilité, protection de la vie privée, etc. Les systèmes de chaque type mettent ces propriétés en œuvre en fonction du contexte spécifique de leur utilisation. Dans tous les cas, il s'agit de contraintes de premier plan pour le concepteur comme pour l'utilisateur.

Certains agents conversationnels provoquent des tensions éthiques nouvelles, par exemple liées à l'impossibilité d'expliquer en langue naturelle la chaîne des décisions aboutissant à telle ou telle recommandation médicale. Des préconisations sont formulées à cet égard dans l'avis de la CERNA sur les questions éthiques de la recherche en apprentissage machine[123].

[123] http://cerna-ethics-allistene.org/Publications%2bCERNA/apprentissage/index.html

CONSULTATION

I. Les facteurs éthiques dans l'utilisation des chatbots

1) Confusion de statut. Plusieurs facteurs contribuent à faire confondre un agent conversationnel avec un être humain. Un effacement des distinctions de statut peut advenir comme une brève illusion ou, au contraire, il peut persister tout au long d'un dialogue. Il peut également être volontaire ou spontané, avoir des conséquences psychologiques ou juridiques, donner lieu à des manipulations plus ou moins graves. Cette confusion de statut a pour cause un phénomène plus général.

Quelle que soit la nature de son interlocuteur, l'être humain projette sur lui spontanément des traits humains : pensée, volonté, désir, conscience, représentation interne du monde. Ce comportement est qualifié d'« anthropomorphisme ». L'interlocuteur apparaît alors comme un individu autonome doté de pensée propre, qu'il exprime à travers sa parole.

A ce jour, seule une loi de l'État de Californie[124] impose explicitement de mentionner l'existence d'une interaction avec un chatbot lorsque cette interaction entend inciter à l'achat ou vendre des produits ou services dans le cadre d'une transaction commerciale ou influencer le vote dans un cadre électoral. Il n'existe pas d'équivalent à cette disposition dans le droit français ou européen même si une réflexion est désormais engagée sur ce point[125].

1.1 Faut-il informer l'utilisateur de la nature de son interlocuteur (être humain ou machine) ? Si oui, quelles informations sur le chatbot faut-il communiquer à l'utilisateur (finalités, corpus d'entraînement, nom du concepteur, etc.) ?

1.2. Pensez-vous qu'en Europe, il faudrait adopter un cadre législatif comparable à celui de l'État de Californie ?

1.2 Remarque libre :

2) Attribution de nom propre. Souvent, l'être humain donne à un agent conversationnel un nom, comme par exemple les enfants le font avec leurs poupées.

Parfois, l'attribution du nom est voulue par le concepteur : s'adresser à la machine par un nom peut aider à mieux réaliser sa fonction, par exemple dans les secteurs d'assistance aux personnes ou de divertissement. Dans ces cas, l'utilisation du nom renforce la réaction émotionnelle de l'utilisateur.

124 https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=BPC&division=7.&title=&part=3.&chapter=6.&article

125 High-Level Expert Group on Artificial Intelligence | Shaping Europe's digital future

Actuellement, ce recours au nom et à la réaction émotionnelle sert encore souvent à masquer le manque de performances sémantiques et contextuelles des agents conversationnels. Attribuer un nom à la machine relève de la dynamique de projection, c'est-à-dire d'anthropomorphisation de cette machine. Or, lorsque l'agent conversationnel lui-même emploie son « nom » dans un dialogue, se pose alors la question de l'autoréférence : à qui ou quoi exactement renvoie ce nom ?

2.1 L'utilisateur devrait-il pouvoir choisir le nom et le genre du nom (masculin, féminin, neutre) porté par un chatbot ou ce choix relève-t-il du concepteur ?

2.2 Un chatbot pourrait-il ou devrait-il se voir attribuer un nom humain (par exemple « Sophia »), un nom non-humain (par exemple « R2D2 ») ou bien aucun nom ?

2.3 Remarque libre :

3) Malmener les chatbots. La projection des qualités humaines sur les agents conversationnels est un phénomène courant et important. En particulier, les utilisateurs pourraient maltraiter un agent conversationnel.

Tandis que votre chatbot vous rappelle les gestes barrière pendant une épidémie, vous pourriez réagir en l'insultant ou en lui ordonnant de se taire. En outre, cela pourrait avoir une incidence sur les enfants qui entendent cet échange.

Les assistants vocaux généralistes (Siri, etc.) se font parfois insulter par les utilisateurs. Dans ce cas, ils répondent selon des stratégies prédéterminées par leurs concepteurs.

3.1 Insulter un chatbot dans une conversation est-ce un acte moralement répréhensible ? Pensez-vous qu'il est admissible de se servir du chatbot comme un souffle-douleur ?

3.2 Un chatbot insulté par son interlocuteur devrait-il pouvoir répondre à l'utilisateur en l'insultant au retour ?

3.3 Si un chatbot répondant à un nom féminin voire ayant une voix féminine est malmené, y voyez-vous un geste de maltraitance envers les femmes ? La même question se pose pour les noms masculins.

3.4 Remarque libre :

4) Confiance dans les chatbots. Une certaine confiance de l'utilisateur envers les finalités du chatbot est nécessaire pour la réalisation des tâches fonctionnelles du chatbot.

La confiance n'est pas seulement un phénomène psychologique émergent mais relève d'un effort technique : les concepteurs des agents conversationnels cherchent à l'établir et à la maintenir, mais pourraient également se poser la question d'éviter qu'elle soit accordée au chatbot de manière irréfléchie.

L'évaluation du niveau de confiance des utilisateurs envers les comportements et performances du chatbot est un important sujet de recherche.

4.1 Si la réponse « je ne sais pas » d'un chatbot vient en conflit avec la préservation de la confiance de l'utilisateur, par exemple dans le cas d'un service après-vente, faut-il privilégier la confiance en modifiant la réponse ?

4.2 Afin de gagner la confiance, le chatbot peut-il se présenter comme un.e « assistant.e / conseiller.ère / ami.e » de l'utilisateur ?

4.3 Remarque libre :

5) Les conflits des chatbots. Si la plupart des systèmes de dialogue sont conçus pour une tâche spécifique, de nombreux autres sont des agents conversationnels généralistes. Leur interaction avec l'être humain peut participer à un conflit. On se pose alors la question du rôle de l'agent conversationnel dans ce conflit et du jugement qui va tomber sur lui. *Par exemple, un chatbot pourrait donner de fâcheux conseils à son utilisateur, lui mentir, ou encore se comporter en délateur en appelant la police s'il détecte à tort ou à raison une menace.*

Les recherches actuelles portent sur le développement et l'utilisation des systèmes capables de s'adapter aux utilisateurs, à leurs desiderata, intentions et croyances en leur répondant comme le ferait un proche. Ces réponses adaptées voire « intelligentes » en réaction aux questions ou comportements des humains ne peuvent qu'engendrer chez les utilisateurs des croyances sur des « compétences » ou des supposés « états d'esprit » de la machine. L'humain s'adapte ainsi aux agents conversationnels avec lesquels il dialogue, soit en s'en méfiant, soit au contraire en leur donnant un certain « crédit de vérité ». En s'appuyant sur son « crédit de vérité », un chatbot pourrait proférer un mensonge.

La tension émerge lorsque le chatbot, par exemple, répond à une question de l'utilisateur relative à sa santé. Un médecin peut le cas échéant cacher toute la vérité à son patient dans le souci du bien-être de celui-ci.

5.1 Le mensonge proféré par un chatbot est-il plus ou moins acceptable que le mensonge humain ? La réponse dépend-elle du contexte (assistant vocal, éducation, psychothérapie, recrutement, etc.) ?

5.2 Si les chatbots peuvent mentir aux utilisateurs, qui et comment devrait décider des buts admissibles et des limites de tels comportements ?

5.3 Remarque libre :

6) La manipulation (*nudge*) des chatbots. Prix Nobel d'économie, l'Américain Richard Thaler a mis en lumière le concept de nudge, qui consiste à inciter les individus à changer de comportement sans les contraindre, par la seule utilisation de leurs biais cognitifs. Dans le cas des chatbots, les nudges sont définis comme des suggestions ou manipulations, manifestes ou cachées, conçues pour influencer le comportement ou les émotions d'un utilisateur.

Les agents conversationnels pourraient ainsi devenir un moyen d'influence des individus à des fins mercantiles ou politiques. Mais le nudge est aussi souvent mis en œuvre pour surveiller notre santé ou pour améliorer notre bien-être (faire plus d'exercice physique, consommer moins d'alcool, arrêter de fumer, etc.).

6.1 Tous les nudges sont-ils permis ? Comment peut-on distinguer les bons des mauvais nudges ?

6.2 Le concept de consentement libre et éclairé dans le cadre d'un agent conversationnel capables de « nudge » a-t-il encore un sens ?

6.3 Remarque libre :

7) Les chatbots et le libre choix. Lors d'un dialogue, les chatbots évaluent plusieurs réponses possibles pour en donner une seule. Dans le cas des systèmes de recommandation, ce choix unique pourrait limiter la liberté de l'utilisateur de choisir de manière autonome, en dérobant à sa vue toute la palette d'options disponibles. Cela génère en outre un risque d'enfermement (*filter bubble*), problème renforcé par le faible niveau de paramétrage proposé par les systèmes commercialisés actuellement.

Par exemple, à la demande de commander une pizza, le chatbot propose de commander chez un restaurateur particulier. Cela peut être le fournisseur plus proche géographiquement, le mieux noté sur un site donné ou encore celui qui possède un accord commercial avec le concepteur du chatbot. Or il propose un choix unique tandis qu'il existe

au voisinage quinze pizzerias qui proposent le service demandé. Ce choix unique peut poser un problème éthique lié à la liberté et à la discrimination.

7.1 Dans l'exemple cité, souhaiteriez-vous que le chatbot explicite tous les choix ou plusieurs choix ?

7.2 Pensez-vous qu'une information transparente de l'utilisateur sur les critères de choix des recommandations par le chatbot soit une solution satisfaisante aux problèmes éthiques du libre choix et de la discrimination ?

7.3 Remarque libre :

8) Les émotions des chatbots. Les émotions sont souvent mélangées dans la vie de tous les jours. En conséquence, la détection et l'identification des émotions des utilisateurs dépendent d'un grand nombre de facteurs contextuels, culturels et idiosyncrasiques. L'informatique émotionnelle comprend trois grands domaines : détecter les émotions des humains, raisonner sur ces informations pour modifier la stratégie du dialogue et générer une expressivité émotionnelle par le langage ou le comportement non-verbal du chatbot.

Par exemple, ayant reconnu que l'utilisateur est stressé, un agent conversationnel peut simuler l'empathie et exprimer la compréhension de l'état de l'utilisateur.

8.1 Est-il souhaitable de construire des chatbots qui détectent les émotions des êtres humains ? Précisez la réponse selon le contexte d'utilisation.

8.2 Est-il souhaitable de construire des chatbots qui simulent des émotions des êtres humains ? Précisez la réponse selon le contexte d'utilisation.

8.3 Remarque libre :

9) Les chatbots et les personnes vulnérables. Un chatbot peut occuper toute l'attention d'une personne vulnérable en remplaçant, comme dans le cas des enfants autistes, le difficile contact avec les personnes humaines. Ce phénomène provoque souvent des jugements polarisés : d'un côté, le bien-être de la personne peut être amélioré ; de l'autre, il l'est au dépens de sa socialisation humaine « standard ».

Par exemple, un enfant autiste pourrait préférer l'interaction très nourrie et prolongée avec un chatbot à celle avec un parent ou un pédagogue. Un jeune enfant pourrait apprendre et imiter les comportements émotionnels de la machine au lieu de ceux des humains. Une personne âgée pourrait vouloir faire le deuil de son chatbot ou l'enterrer si elle lui est très attachée et qu'il ne fonctionne plus.

9.1 Quelles finalités de l'interaction entre un chatbot et une personne vulnérable (surveillance, éducation, accompagnement, divertissement) sont acceptables ? La réponse dépend-elle de l'âge de la personne (enfant, personne âgée) ou de son statut (patient, personne en convalescence) ?

9.2 Les utilisateurs, notamment les personnes vulnérables, sont susceptibles de s'attacher profondément à des chatbots, ce qui peut entraîner une modification durable de leur façon de vivre ou de leurs interactions sociales. Ce phénomène est-il inquiétant ? Pourquoi ?

9.3 Remarque libre :

10) Les chatbots et la mémoire des morts. Si le droit à la vie privée s'éteint à la mort de la personne, l'utilisation post-mortem de ses données, par exemple de sa voix, par un chatbot pour faire « revivre » cette personne peut néanmoins poser problème quant à l'atteinte possible au principe de respect de la dignité de la personne humaine.

Un journaliste américain est parvenu à créer un chatbot, le « dadbot », à partir des souvenirs qu'il avait de son père[126]*. Il échange avec ce chatbot « comme si » il s'agissait d'un échange avec son père.*

10.1 Pensez-vous que les chatbots sont un moyen envisageable pour faire « vivre » la mémoire ou la manière de s'exprimer propres à une personne décédée ? De tels usages porteraient-ils atteinte au principe de respect de la dignité de la personne humaine ?

10.2 Quelle évolution du concept de mort envisagez-vous en tenant compte des possibilités offertes par les chatbots ?

10.3 Remarque libre :

11) Surveillance par les chatbots. Si certains chatbots font partie des systèmes exclusivement consacrés à l'interaction humain-machine, d'autres fonctionnent dans des environnements partagés. Les chatbots capables d'enregistrer la voix pourraient ainsi surveiller les interactions autour d'eux, que celles-ci soient humaines ou avec d'autres chatbots. Cette capacité implique des enjeux éthiques et juridiques liées à la protection de la vie privée, à l'exploitation des données personnelles sans consentement, au risque de violation du secret personnel ou professionnel ainsi qu'à l'introduction de failles de

[126] James Vlahos. *Talk to me, Amazon, Google, Apple, and the Race for Voice-Controlled AI*. Random House, 2019.

sécurité. La divulgation par les chatbots des contenus enregistrés à l'insu des personnes peut s'apparenter à la délation.

Par exemple, en cas d'écart à la diète que le médecin a imposée à un patient, le chatbot l'en informe, voire se met en contact l'organisme de soins de santé.

Autre exemple, un chatbot peut « tenir compagnie » des personnes vulnérables ou âgées en surveillant leur comportement.

11.1 Dans les exemples cités, pensez-vous que le comportement du chatbot est justifié ? Comment, dans ce cas, l'utilisateur peut-il exprimer son consentement ? Qu'en est-il si les chatbots sont placés dans des espaces partagés ?

11.2 Donnez d'autres exemples de situation dans laquelle la surveillance par un chatbot vous paraît justifiée.

11.3 Si un chatbot est insulté par son utilisateur, cette information doit-elle être communiquée par le chatbot à une tierce partie, par exemple son concepteur ?

11.4 Remarque libre :

12) Les chatbots et le travail. Les chatbots présenteront des opportunités et des risques pour les entreprises selon les contextes de leur utilisation (évaluation, recrutement, divertissement, etc.). L'introduction d'agents conversationnels dans les équipes peut induire des effets organisationnels selon les secteurs industriels, notamment du point de vue de la charge informationnelle et émotionnelle, de la temporalité du travail, du sentiment de cohésion ou d'isolement des travailleurs, des effets des chatbots sur le moral des employés ainsi que les problèmes d'égalité et de reconnaissance au mérite au sein des entreprises.

Par exemple, dans le secteur médical, l'aide à l'action humaine (médecins psychiatres, médecins généralistes, infirmiers, agents des centres d'appel d'urgence, etc.) par des chatbots pourrait provoquer des effets sur la profession dans sa totalité ainsi que sur le bien-être des patients et des personnels soignants et sur la relation entre eux.

12.1 Existe-t-il des métiers ou des pratiques humaines dans lesquels le recours aux chatbots devrait être encouragé ou prohibé ?

12.2 Comment et à quelle échelle temporelle envisagez-vous l'évolution des métiers à la suite de l'introduction des chatbots ? Précisez votre réponse selon un ou plusieurs cas d'usage.

12.3 Par quels moyens (législatif, code de bonne conduite, etc.) le recours aux chatbots devrait-il être encadré ?

12.4 Remarque libre :

13) Effets à long terme sur le langage. À moyen et long termes, l'utilisation des chatbots peut avoir une incidence durable sur le langage humain et peut-être également sur les habitudes de vie.

Par exemple, si les chatbots répondent par des phrases courtes, linguistiquement pauvres, sans politesse aucune, les humains risquent d'imiter ces tics langagiers lorsqu'ils s'adressent à d'autres humains.

13.1 Comment envisagez-vous l'évolution du langage sous l'influence des chatbots ? Cette influence peut-elle être jugée comme bonne ou mauvaise ?

13.2 Quelle échelle temporelle peut-on envisager pour cette évolution ?

13.3 Remarque libre :

II. Les facteurs éthiques dans la conception des chatbots

14) **Problème de spécification.** Les lois et les règles de conduite dans la société sont formulées dans une langue naturelle. Leur traduction dans un langage informatique exige une « spécification » : définition de tous les termes dans un cadre formel. Souvent, la spécification complète est impossible : par exemple, le terme « humain » peut inclure des humains qui seraient facilement identifiables par un système informatique apprenant, mais aussi des humains que le système ne parviendra pas à identifier comme tels car absents des données d'apprentissage. Quels que soient la base d'apprentissage et l'algorithme déployé, les erreurs d'identification sont inévitables : par nature, la langue humaine admet la multiplicité des significations.

Pour les chatbots, le problème de spécification se traduit, par exemple, par la difficulté de distinguer systématiquement et sans erreur, l'usage ironique ou satirique d'un concept ou d'une expression de son usage indicatif standard.

14.1 Quelles erreurs commises par les chatbots seraient acceptables et lesquelles ne le seraient pas ? Précisez la réponse selon le contexte (santé, éducation, divertissement, service après-vente, etc.).

14.2 Si un chatbot n'est pas capable de trouver une réponse, doit-il le dire explicitement ?

14.3 Quelles conséquences sur le comportement des utilisateurs la réponse « je ne sais pas », fréquemment donnée par les assistants vocaux actuels, entraîne-t-elle ? Si vous avez vécu cette expérience, décrivez-la.

14.4 Remarque libre :

15) **Les métriques et les fonctions d'évaluation.** Dans un agent conversationnel, les fins recherchées par le concepteur donnent lieu à la définition d'une métrique ou d'une fonction d'évaluation, qui quantifie la mesure de « bonne réponse » ou « réplique adéquate » pour le système. Cette métrique est encodée au préalable. La métrique d'un chatbot peut aussi tenir compte des facteurs émergents, qui apparaissent pendant la conversation, par ailleurs susceptibles de causer des ruptures dans la compréhension humaine du comportement du système. Souvent, cette qualité du dialogue est mesurée par le degré d'engagement de l'utilisateur, c'est-à-dire sa volonté à poursuivre le dialogue avec le chatbot. La métrique d'engagement utilise la longueur des échanges comme des marqueurs paralinguistiques (rire, sourire, hésitation, hochement de tête, etc.) de satisfaction ou d'intérêt ; or, dans l'état actuel des recherches, elle tient rarement compte du contenu sémantique des échanges. Cela peut défavoriser ceux qui ne comprennent pas le procédé d'évaluation de l'agent conversationnel et en outre donner lieu à des comportements manipulateurs de la part des utilisateurs.

En avril 2016, le chatbot Tay *de* Microsoft*, qui avait la capacité d'apprendre en continu à partir de ses interactions avec les internautes, avait appris à tenir des propos racistes.* Tay *a été rapidement retiré par* Microsoft*.*

Malgré cette expérience, DeepCom*, un autre chatbot développé par* Microsoft China *en 2019 afin de commenter des nouvelles sur les réseaux sociaux, a été reconnu par ses concepteurs eux-mêmes comme étant susceptible de générer des contenus biaisés, (par exemple, discriminants) voire de la propagande, à la suite de fortes réactions dans la communauté de recherche*[127]*. La première version de la publication postulait : « Compte tenu de la prévalence des articles de presse en ligne avec commentaires, il est très intéressant de mettre en place un système de commentaire automatique des nouvelles avec des approches construites à partir des données ». Dans la version révisée, les auteurs affirment : « Il existe un risque que des personnes et des organisations utilisent ces techniques à grande échelle pour simuler des commentaires provenant de personnes à des fins de manipulation ou de persuasion politique ».*

15.1 Faudrait-il que l'utilisateur soit informé du fait que la stratégie de dialogue d'un chatbot puisse être adaptée au cours de la conversation ?

15.2 Comme expliqué plus haut, l'utilisateur peut manipuler la métrique d'un chatbot à ses propres fins. S'il le fait, le concepteur partage-t-il l'éventuelle responsabilité pour les résultats de cette manipulation ou devrait-il en être dédouané ?

15.3 Avez-vous vécu des exemples personnels liés, selon votre interprétation, aux métriques particulières des chatbots ?

15.4 Remarque libre :

16) Les finalités de l'agent conversationnel : Les finalités d'un chatbot, c'est-à-dire les buts qui lui sont assignés, sont définies par ses concepteurs, et le chatbot cherche à les satisfaire dès sa mise en marche. Si cela ne pose pas de problèmes excessifs pour les chatbots dédiés à une ou plusieurs tâches connues au préalable, la spécification des finalités peut s'avérer complexe pour un chatbot généraliste car elles ne sont pas toutes énumérables au moment de la conception.

Ces finalités peuvent être très diverses : des systèmes après-vente aident à réparer des produits défectueux, des conseillers médicaux cherchent à améliorer l'état du patient, des services d'aide au recrutement, etc.

D'autres systèmes possèdent des finalités plus vagues : certains chatbots sont conçus afin de converser librement avec l'utilisateur sur tous les sujets. Que la perception des finalités ou le jugement que l'on porte sur elles puissent évoluer, cela ne supprime guère cette

[127] Microsoft Used Machine Learning to Make a Bot That Comments on News Articles For Some Reason

distinction fondamentale entre un agent conversationnel et un humain qui peut agir sans finalité prédéterminée et peut ne pas rendre sa finalité transparente aux autres.

16.1 Doit-on révéler la finalité d'un chatbot à l'utilisateur ? Si oui, à quel moment et sous quelle forme ? Si non, pourquoi ?

16.2 Devrait-on accepter qu'un chatbot capable d'apprentissage en interaction (par exemple, un agent conversationnel généraliste) puisse être dirigé vers une finalité particulière à travers une influence intentionnelle ou involontaire de la part des utilisateurs (par exemple, inciter la personne à faire un don ou à acheter un produit particulier) ? Précisez la réponse selon le contexte (santé, éducation, divertissement).

16.3 Remarque libre :

17) Les biais d'apprentissage. Un système apprend à partir de données sélectionnées par un « entraîneur » (agent humain responsable de leur sélection). L'existence de biais dans les données d'apprentissage est une source majeure des conflits éthiques, notamment à travers la discrimination ethniques, culturelles ou encore de genre.

Par exemple, des données de parole enregistrées peut contenir uniquement des voix d'adultes alors que le système est censé interagir aussi avec les enfants, ou un corpus de textes peut utiliser statistiquement plus fréquemment des pronoms de genre féminin que ceux de genre masculin.
Le système reproduira alors ces biais issus d'un corpus d'apprentissage, sauf s'il est équipé d'outils spécialement conçus dans le but de les corriger, ce qui présuppose déjà la connaissance des biais possibles. Or, certains biais pourraient ne pas être connus à l'avance.

17.1 Considérez-vous qu'un agent conversationnel devrait être sans biais ? Est-ce possible ? Précisez la réponse selon le contexte (santé, recrutement, service après-vente, éducation, sécurité, assistant vocal domestique).

17.2 Pensez-vous que les chatbots devraient imiter les biais humains ou les corriger ?

17.3 Remarque libre :

18) Instabilité de l'apprentissage. Des erreurs sont inévitables lorsqu'un système apprenant classifie une donnée qui ne ressemble pas, ou qui ressemble faussement, à celles contenues dans le corpus utilisé pendant son apprentissage. Dans le cas des agents conversationnels, cela recouvre les homophones, homographes, homonymes ou autres exemples d'ambiguïté linguistique.

Un cas simple est celui des erreurs d'orthographe : le comportement du chatbot dans ce cas diffère totalement de celui de l'être humain. Par exemple, l'utilisateur humain reconnaît un mot même s'il contient plusieurs erreurs, tandis qu'à cause de l'instabilité, un algorithme cesse de reconnaître correctement un mot contenant une ou deux fautes d'orthographe.

18.1 L'apprentissage des chatbots étant instable, il induit des erreurs parfois évidentes. Êtes-vous prêt à tolérer ces erreurs davantage que les erreurs humaines ? Précisez la réponse selon le contexte.

18.2 Les erreurs des chatbots provoquent-elles des sentiments ou des réactions différentes par rapport aux erreurs humaines ? Lesquelles ?

18.3 Remarque libre :

19) Explicabilité et transparence. La transparence d'un système signifie que son fonctionnement n'est pas opaque ou incompréhensible pour l'homme. Elle s'appuie notamment sur la traçabilité des répliques sélectionnées par un agent conversationnel. L'explicabilité signifie qu'un utilisateur peut appréhender le comportement du chatbot. Les problèmes de transparence et d'explicabilité sont provoqués par différents facteurs, notamment par le fait que, contrairement à l'être humain, un système informatique ne comprend pas le sens des phrases qu'il génère ou qu'il perçoit.

Ainsi, un chatbot, qui n'a pas de représentation du monde, *est susceptible de formuler des phrases qui ne correspondent à aucune réalité (« lait noir »), de répondre sans tenir compte du contexte (« Comment vas-tu ? » - « Il fait beau ») ou d'employer un lexique désagréable ou prohibé*.

Les effets immédiats sur l'utilisateur provoqués par un tel dialogue peuvent être importants (réaction émotionnelle forte, rupture dans la compréhension, abandon du dialogue ou débranchement du système). La question de responsabilité se pose alors à l'égard des concepteurs et des entraîneurs des agents conversationnels. La dimension esthétique (certaines paroles peuvent être étranges mais belles) suffit-elle à dédouaner le chatbot du besoin d'imiter toujours la parole humaine ?

19.1 À quelle réaction peut-on s'attendre de la part d'un utilisateur en situation de rupture de compréhension dans un dialogue avec le chatbot ? Précisez la réponse selon les finalités de celui-ci et le contexte (par exemple, santé, assistant vocal généraliste, divertissement, recrutement).

19.2 Lorsque l'utilisateur donne spontanément un sens à des répliques peu compréhensibles du chatbot, ce phénomène relève-t-il d'une attitude ludique ou pose-t-il un problème éthique ?

19.3 Remarque libre :

20) Impossibilité d'évaluation rigoureuse. Un agent conversationnel fournit une réponse en appliquant des stratégies de dialogue qui dépendent de l'interprétation. Les modèles les plus avancés utilisent de grands corpus de données pour apprendre.

L'évaluation de ce système de dialogue, par essence dynamique, est difficile au moins sur deux plans : *a) la prédiction des entrées générées par l'utilisateur n'est souvent pas possible; b) les aléas de l'apprentissage contribuent à la difficulté de reproduire le comportement du système*.

Or, l'incertitude théorique et pratique va de pair avec les techniques d'apprentissage qui procurent aux systèmes leur grande efficacité.

20.1 Est-ce acceptable qu'un chatbot profère des phrases « incongrues », qu'aucun être humain n'a jamais utilisées, ce qui serait susceptible d'influencer son interlocuteur ?

20.2 Un chatbot devrait-il se limiter à un ensemble prédéterminé de phrases ou, à l'inverse, en générer librement ? Précisez la réponse selon le contexte (divertissement, service après-vente, éducation, assistant vocal généraliste).

20.3 Remarque libre :

Merci beaucoup pour votre contribution !

L'envoi se fait à l'adresse cnpen-consultation-chatbots@ccne.fr

66, rue de Bellechasse 75007 Paris – 01 42 75 66 42
www.ccne.fr – contact@comite-ethique.fr